

Barricade™ Plus

Wireless Cable/DSL Broadband Router with VPN

Wireless Cable/DSL Broadband Router with VPN

- ◆ EZ 3-Click Installation Wizard
- ◆ IEEE 802.11b Compliant
- ◆ Wireless Operation at 11, 5.5, 2, or 1 Mbps
- ◆ Internet Access via –
 - 10/100 Mbps WAN port connection to xDSL/Cable modem
- ◆ Home Networking via –
 - Three 10/100 Mbps Ethernet switch ports with MDI/MDI-X auto-negotiation
- ◆ Configurable Parental Control by limiting access to web sites with URL and keyword blocking
- ◆ Stateful Packet Inspection (SPI) Advanced Firewall Protection
- ◆ Client Privileges, Intrusion Detection, NAT
- ◆ Built-in VPN Tunneling Capability



BarricadeTM Plus Wireless Cable/DSL Broadband Router User Guide

From SMC's Barricade line of Broadband Routers

SMC[®]

Networks

38 Tesla

Irvine, CA 92618

Phone: (949) 679-8000

May 2002
Revision Number: R01

Copyright

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2002 by
SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

All rights reserved. Printed in Taiwan

Trademarks:

SMC is a registered trademark; and Barricade is a trademark of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

LIMITED WARRANTY

Limited Warranty Statement: SMC Networks, Inc. (“SMC”) warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an “Active” SMC product. A product is considered to be “Active” while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an “Active” SMC product. A list of discontinued products with their respective dates of discontinuance can be found at: http://www.smc.com/index.cfm?action=customer_service_warranty.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

LIMITED WARRANTY

WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

COMPLIANCES

FCC - Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with instructions, may cause harmful interference to radio communications. However, there is no guarantee that the interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CAUTION STATEMENT: FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

EC Conformance Declaration - Class B

SMC contact for these products in Europe is:

SMC Networks Europe,
Edificio Conata II,
Calle Frutuós Gelabert 6-8, 2^o, 4^a,
08970 - Sant Joan Despí,
Barcelona, Spain.

This information technology equipment complies with the requirements of the Council Directive 89/336/EEC on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility and 73/23/EEC for electrical equipment used within certain voltage limits and the Amendment Directive 93/68/EEC. For the evaluation of the compliance with these Directives, the following standards were applied:

- RFI * Limit class B according to EN 55022:1998
- Emission: * Limit class A for harmonic current emission according to EN 61000-3-2/1995
- * Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3/1995
- Immunity: * Product family standard according to EN 55024:1998
- * Electrostatic Discharge according to EN 61000-4-2:1995 (Contact Discharge: ± 4 kV, Air Discharge: ± 8 kV)
- * Radio-frequency electromagnetic field according to EN 61000-4-3: 1996 (80 - 1000MHz with 1kHz AM 80% Modulation: 3V/m)
- * Electrical fast transient/burst according to EN 61000-4-4:1995(AC/DC power supply: ± 1 kV, Data/Signal lines: ± 0.5 kV)
- * Surge immunity test according to EN 61000-4-5:1995(AC/DC Line to Line: ± 1 kV, AC/DC Line to Earth: ± 2 kV)
- * Immunity to conducted disturbances, Induced by radio-frequency fields: EN 61000-4-6:1996(0.15 - 80MHz with 1kHz AM 80% Modulation: 3V/m)
- * Power frequency magnetic field immunity test according to EN 61000-4-8:1993(1A/m at frequency 50Hz)
- * Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994(>95% Reduction @10ms, 30% Reduction @500ms, >95% Reduction @500ms)
- LVD: * EN60950(A1/1992; A2/1993; A3/1993; A4/1995; A11/1997)

Industry Canada - Class B

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par le ministère des Communications.

Japan VCCI Class B

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境でを使用することを目的としています。この装置がラジオやテレビジョン受信機に近接して使用されると受信障害を引き起こすことがあります。

取り扱い説明書に従って正しい取り扱いをして下さい。

Australia AS/NZS 3548 (1995) - Class B



ACN 069 351 613

SMC contact for products in Australia is:

SMC Communications Pty. Ltd.
Suite 18, 12 Tryon Road,
Lindfield NSW2070,
Phone: 61-2-94160437
Fax: 61-2-94160474

Safety Compliance

Underwriters Laboratories Compliance Statement

Important! Before making connections, make sure you have the correct cord set. Check it (read the label on the cable) against the following:

Operating Voltage	Cord Set Specifications
120 Volts	UL Listed/CSA Certified Cord Set
	Minimum 18 AWG
	Type SVT or SJT three conductor cord
	Maximum length of 15 feet
	Parallel blade, grounding type attachment plug rated 15A, 125V
240 Volts (Europe only)	Cord Set with H05VV-F cord having three conductors with minimum diameter of 0.75 mm ²
	IEC-320 receptacle
	Male plug rated 10A, 250V

The unit automatically matches the connected input voltage. Therefore, no additional adjustments are necessary when connecting it to any input voltage within the range marked on the rear panel.

Wichtige Sicherheitshinweise (Germany)

1. Bitte lesen Sie diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine flüssigkeits- oder aerosolhaltigen Reiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung.
4. Die Netzanschlusssteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Beschädigungen hervorrufen.
7. Die Lüftungsöffnungen dienen der Luftzirkulation, die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Verlegen Sie die Netzanschlusleitung so, daß niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
10. Alle Hinweise und Warnungen, die sich am Gerät befinden, sind zu beachten.
11. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das

- Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
13. Öffnen sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von autorisiertem Servicepersonal geöffnet werden.
 14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
 - a. Netzkabel oder Netzstecker sind beschädigt.
 - b. Flüssigkeit ist in das Gerät eingedrungen.
 - c. Das Gerät war Feuchtigkeit ausgesetzt.
 - d. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
 - e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
 - f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
 15. Stellen Sie sicher, daß die Stromversorgung dieses Gerätes nach der EN 60950 geprüft ist. Ausgangswerte der Stromversorgung sollten die Werte von AC 7,5-8V, 50-60Hz nicht über oder unterschreiten sowie den minimalen Strom von 1A nicht unterschreiten..
- Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70dB(A) oder weniger.

COMPLIANCES

TABLE OF CONTENTS

1	Introduction	1-1
	About the Wireless Barricade Plus	1-1
	Features and Benefits	1-2
	Applications	1-3
2	Installation	2-1
	Package Contents	2-1
	Description of Hardware	2-2
	System Requirements	2-4
	Connect the System	2-5
	Basic Installation Procedure	2-6
	Verify Port Status	2-11
3	Configuring Client PCs	3-1
	TCP/IP Configuration	3-1
4	Configuring the Wireless Barricade Plus	4-1
	Navigating the Web Browser Interface	4-2
	Making Configuration Changes	4-3
	Setup Wizard	4-3
	Broadband Type	4-3
	Advanced Setup Menu	4-7
	Navigating the Web Browser Interface	4-7
	Main Menu	4-8
	Making Configuration Changes	4-10
	System Settings	4-11
	Set Time Zone	4-11
	Setting a Password	4-12
	Remote Management	4-13
	Networking and Client Services	4-14
	WAN Configuration	4-14
	DNS Configuration	4-18

TABLE OF CONTENTS

	LAN Gateway and DHCP Settings	4-19
	Wireless Configuration	4-20
	Configuring Client Services	4-25
5	Configuring Client TCP/IP	5-1
	Installing TCP/IP Protocol in Your PC	5-1
	Windows 95/98/ME	5-1
	Windows 2000	5-3
	Setting TCP/IP to Work with the Wireless Barricade Plus	5-5
	Windows 95/98/ME	5-5
	Windows 2000	5-6
	Windows XP	5-7
	Configuring Your Computer with Windows 95/98/ME	5-8
	Configuring Your Computer with Windows 2000	5-15
	Configuring Your Computer with Windows XP	5-22
	Configuring Your Computer with Windows NT 4.0	5-29
	Configuring Your Macintosh Computer	5-36
	Dynamic IP Allocation via a DHCP Server	5-43
	Manual IP Configuration	5-44
	Verifying Your TCP/IP Connection	5-45
A	Troubleshooting	A-1
B	Cables	B-1
	Ethernet Cable	B-1
	Specifications	B-1
	Twisted-pair Cable	B-1
	RJ-45 Port Pin Assignments	B-3
C	Specifications	C-1
D	Ordering Information	D-1

CHAPTER 1

INTRODUCTION

Congratulations on your purchase of the Barricade™ Plus Wireless Cable/DSL Broadband Router. SMC is proud to provide you with a powerful yet simple communication device for connecting your local area network (LAN) to the Internet. For those who want to surf the Internet in the most secure way, this Wireless Cable/DSL Broadband Router provides a convenient and powerful solution.

About the Wireless Barricade Plus

The Wireless Barricade Plus provides Internet access to multiple users by sharing a single-user account. It serves as a wireless Access Point, and includes a 10/100Mbps WAN port which allows you to connect to an xDSL or Cable modem. The most outstanding feature of the Wireless Barricade Plus is its extensive firewall protection and Virtual Private Network (VPN) services.

This new Wireless Barricade Plus technology provides many secure and cost-effective functions. It is simple to configure and can be up and running in minutes.

Features and Benefits

- Internet connection to xDSL or cable modem via a 10/100 Mbps WAN port
- Local network connection via 10/100 Mbps Ethernet ports or 11 Mbps wireless interface (supporting up to 128 mobile users)
- 802.11b Compliant – interoperable with multiple vendors
- Provides seamless roaming within 802.11b WLAN environment
- Supports 64-bit and 128-bit WEP (Wired Equivalent Privacy)
- DHCP for dynamic IP configuration, and DNS for domain name mapping
- Firewall with Stateful Packet Inspection, client privileges, intrusion detection, VPN, and NAT
- NAT also enables multi-user access with a single-user account, and virtual server functionality (providing protected access to Internet services such as Web, FTP, mail and Telnet)
- Supports VPN (Virtual Private Network) tunneling, IPSec and PPTP
- Easy setup through a Web browser on any operating system that supports TCP/IP
- Compatible with all popular Internet applications

Applications

Many advanced applications are provided by the Wireless Barricade Plus, such as:

- **Flexible LAN Access**

The Wireless Barricade Plus provides connectivity to 10/100 Mbps wired devices as well as 11 Mbps wireless mobile users. The wireless interface makes it easy to create a network in difficult-to-wire environments, or to provide quick access to databases for mobile workers.

- **Internet Access**

This device supports Internet access through an xDSL, or Cable connection. Since many DSL providers use PPPoE to establish communications with end users, the Wireless Barricade Plus includes a built-in client for this protocol, eliminating the need to install this service on your computer.

- **Shared IP Address**

The Wireless Barricade Plus provides Internet access for up to 253 users with a shared IP address. Using only one ISP account, multiple users on your network can browse the Web at the same time.

- **Virtual Server**

If you have a fixed IP address, you can set up the Wireless Barricade Plus to act as a virtual host using network address translation (NAT). Remote users access various services at your site using a constant IP address. Then, depending on the requested service (or port number), the Wireless Barricade Plus can route the request to the appropriate server (at another internal IP address). This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network.

- **DMZ Host Support**

Allows a networked computer to be fully exposed to the Internet.

- **Security**

The Wireless Barricade Plus supports security features that can deny Internet access to specified users, or filter all requests for specific services the administrator does not want to serve. The Wireless Barricade Plus' firewall can also block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

- **Stateful Packet Inspection (SPI)**

Stateful Packet Inspection is one of the firewall features provided by the Wireless Barricade Plus. The SPI ensures that the data coming into your network was requested by an end node computer on your network. The Wireless Barricade Plus examines the incoming data and compares it to a database of trusted information. As traffic leaves the network, it is defined by certain characteristics. Incoming information is then compared to these sets of characteristics. If the incoming data matches the predefined set of characteristics,

the incoming traffic is allowed. If no match is found, the incoming traffic is discarded.

- **Virtual Private Network (VPN)**

The Wireless Barricade Plus supports two of the most commonly used VPN protocols – PPTP and IPSec. These protocols allow remote users to establish a secure connection to their corporate network. If your service provider supports VPNs, then any of these protocols can be used to create an authenticated and encrypted tunnel for passing secure data over the Internet (i.e., a traditionally shared data network). The VPN protocols supported by the Wireless Barricade Plus are briefly described below.

- Point-to-Point Tunneling Protocol (PPTP) – Provides a secure tunnel for remote client access to a PPTP security gateway. PPTP includes provisions for call origination and flow control required by ISPs.
- IP Security (IPSec) – Provides IP network-layer encryption. IPSec can support large encryption networks (such as the Internet) by using digital certificates for device authentication.

CHAPTER 2

INSTALLATION

Before installing the Barricade™ Plus Wireless Cable/DSL Broadband Router, verify that you have all the items listed under “Package Contents.” If any of the items are missing or damaged, contact your local SMC distributor. Also be sure that you have all the necessary cabling before installing the Wireless Barricade Plus. After installing the Wireless Barricade Plus, refer to the Web-based configuration program in Chapter 4 for information on configuring the router.

Package Contents

After unpacking The Wireless Barricade Plus Wireless Cable/DSL Broadband Router, check the contents of the box to be sure you have received the following components:

- Barricade Plus Wireless Cable/DSL Broadband Router
- Power adapter 9V 1A
- One CAT-5 Ethernet cable
- Four rubber feet
- Installation CD with EZ 3-Click Installation Wizard, FAQ, Troubleshooting Tips and complete User Guide
- Quick Installation Guide
- SMC Warranty Registration Card

Immediately inform your dealer in the event of any incorrect, missing or damaged parts. If possible, please retain the carton and original packing materials in case there is a need to return the product.

Please fill out and return the Warranty Registration Card to SMC or register on SMC's Web site at www.smc.com. The Wireless Barricade Plus Wireless Cable/DSL Broadband Router is covered by a limited lifetime warranty.

Description of Hardware

The Wireless Barricade Plus can be connected to the Internet or to a remote site using its RJ-45 WAN port. It can be connected directly to your PC or to a local area network using any of the three Fast Ethernet LAN ports or through the wireless interface.

Access speed to the Internet depends on your service type. Full-rate ADSL can provide up to 8 Mbps downstream and 640 Mbps upstream. G.lite (or splitterless) ADSL provides up to 1.5 Mbps downstream and 512 Kbps upstream. Cable modems can provide up to 36 Mbps downstream and 2 Mbps upstream. However, you should note that the actual rate provided by specific service providers may vary dramatically from these upper limits.

Although access speed to the Internet is determined by the modem type connected to your Wireless Barricade Plus, data passing between devices connected to your local area network can run up to 100 Mbps over the Fast Ethernet ports.

The Wireless Barricade Plus includes an LED display on the front panel for system power and port indications that simplifies installation and network troubleshooting. It also provides three RJ-45 LAN ports, one RJ-45 WAN port, as well as two detachable antennas on the rear panel.

- Three RJ-45 ports for connection to a 10BASE-T/100BASE-TX Ethernet Local Area Network (LAN). These ports can auto-negotiate the operating speed to 10/100 Mbps, the mode to half/full duplex, and the pin signals to MDI/MDI-X (i.e., allowing these ports to be connected to any network device with straight-through cable). These ports can be connected directly to a PC or to a server equipped with an Ethernet network interface card, or to a networking device such as an Ethernet hub or switch.
- One RJ-45 port for connection to an xDSL or cable modem. This port is fixed at 10/100 Mbps, full duplex. This port only supports MDI-X pin signals, so you will have to use either straight- through or crossover cable depending on the port type used on the modem.
- Two detachable antennas (dipole, omni-directional).

The following figure shows the components of the Wireless Barricade Plus:

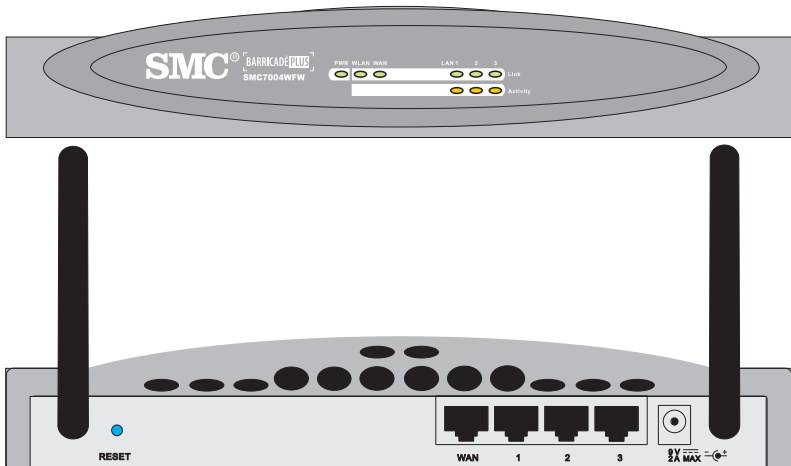


Figure 2-1. Front and Rear Panels

Item	Description
LEDs	Power, WLAN, WAN and LAN port status indicators. (See Verify Port Status on page 2-11.)
Wireless Antennas	Dual antennas provide optimal reception by dynamically choosing the best antenna for each client.
Reset Button	Use this button to reset the power and restore the default factory settings.
WAN Port	WAN port (RJ-45). Connect your Cable modem, xDSL modem, or an Ethernet router to this port.
LAN Ports	Fast Ethernet ports (RJ-45). Connect devices on your local area network to these ports (such as a PC, hub or switch).
Power Inlet	Connect the included power adapter to this inlet. Warning: Using the wrong type of power adapter may cause damage.

System Requirements

You must have an ISP that meets the following minimum requirements:

- Internet access from your Internet Service Provider (ISP) using an xDSL modem, or cable modem.
- A PC using a fixed IP address or dynamic IP address assignment via DHCP, as well as a gateway server address and DNS server address from your service provider.
- For wired LAN connection, you need a computer equipped with a 10 Mbps, 100 Mbps, or 10/100 Mbps Fast Ethernet card, or a USB-to-Ethernet converter. For wireless LAN connections, each computer must have an 11 Mbps wireless adapter.

- TCP/IP network protocol installed on each PC that needs to access the Internet.
- A Java-enabled Web browser, such as Microsoft Internet Explorer 5.0 or above or Netscape Communicator 4.0 or above installed on one PC at your site for configuring the Wireless Barricade Plus.

Connect the System

The Wireless Barricade Plus can be positioned at any convenient location in your office or home. No special wiring or cooling requirements are needed. You should, however, comply with the following guidelines:

- Keep the Wireless Barricade Plus away from any heating devices.
- Do not place the Wireless Barricade Plus in a dusty or wet environment.

You should also remember to turn off the power, remove the power cord from the outlet, and keep your hands dry when you install the Wireless Barricade Plus.

Basic Installation Procedure

1. **Connect the LAN:** You can connect the Wireless Barricade Plus to your PC, or to a hub or switch. Run Ethernet cable from one of the LAN ports on the rear of the Wireless Barricade Plus to your computer's network adapter or to another network device.

You can also connect the Wireless Barricade Plus to your PC (using a wireless client adapter) via radio signals. Position both antennas on the back of the Wireless Barricade Plus into the desired positions. For more effective coverage, you may want to position one antenna along the vertical axis and the other antenna along the horizontal axis. **(The antennas emit signals along the toroidal plane – and thus provide more effective coverage when positioned along alternate axes.)**

2. **Connect the WAN:** Prepare an Ethernet cable for connecting the Wireless Barricade Plus to a cable/xDSL modem or Ethernet router.
3. **Power on:** Connect the power adapter to the Wireless Barricade Plus.

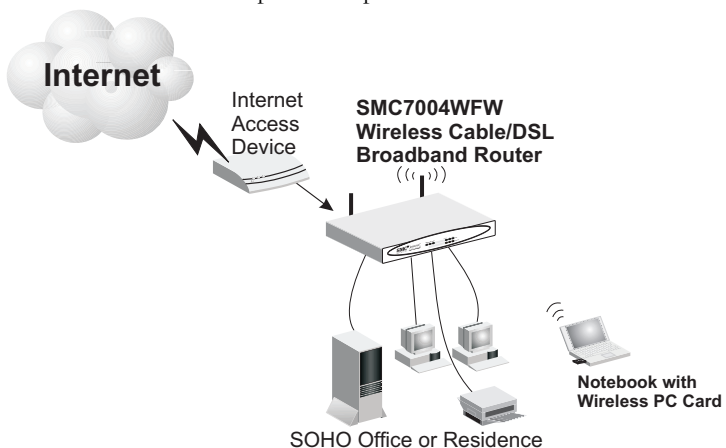


Figure 2-2. Connecting the Wireless Barricade Plus

Attach to Your Network Using Ethernet Cabling

The three LAN ports on the Wireless Barricade Plus can auto-negotiate the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, as well as the transmission mode to half-duplex or full-duplex. These LAN ports also support auto-configuration for pin signals (auto-MDI/MDI-X) that allows you to use straight-through cable for connecting the Wireless Barricade Plus to any network device. (See Appendix B for details on wiring.)

Use twisted-pair cable to connect any of the three LAN ports on the Wireless Barricade Plus to an Ethernet adapter on your PC. Otherwise, you can cascade any of LAN ports on the Wireless Barricade Plus to an Ethernet hub or switch, and then connect your PC or other network equipment to the hub or switch. When inserting an RJ-45 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Warning: Do not plug a phone jack connector into any RJ-45 port. This may damage the Wireless Barricade Plus. Instead, use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

- Notes:**
1. Use 100-ohm shielded or unshielded twisted-pair cable with RJ-45 connectors for all connections. Use Category 3, 4 or 5 for connections that operate at 10 Mbps, and Category 5 for connections that operate at 100 Mbps.
 2. Make sure each twisted-pair cable does not exceed 100 meters (328 feet).

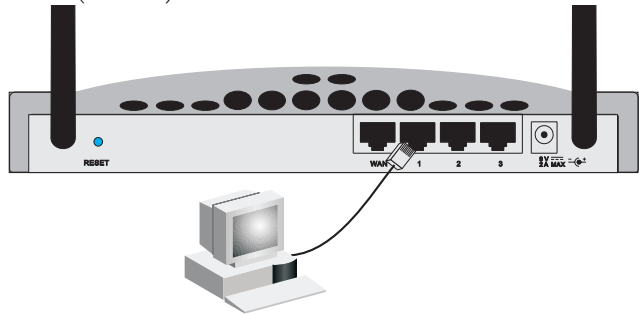


Figure 2-3. Making LAN Connections

Attach to Your Network Using Radio Signals

Install a wireless network adapter in each computer that will be connected to the Internet or your local network via radio signals. SMC currently offers several wireless network cards, including the SMC2602W Wireless PCI card and the SMC2632W Wireless PC card.

Rotate both antennas on the back of the Wireless Barricade Plus to the desired position. For more effective coverage, position one antenna along the vertical axis and the other along the horizontal axis. Try to place the Wireless Barricade Plus in a position that is located in the center of your wireless network. Normally, the higher you place the antenna, the better the performance. Ensure that the Wireless Barricade Plus' location provides optimal reception throughout your home or office.

Computers equipped with a wireless adapter can communicate with each other as an independent wireless LAN by configuring each

computer to the same radio channel. However, the Wireless Barricade Plus can provide access to your wired/wireless LAN or to the Internet for all wireless workstations. Each wireless PC in this network infrastructure can talk to any computer in the wireless group via a radio link, or access other computers or network resources in the wired LAN infrastructure or over the Internet via the Wireless Barricade Plus.

The wireless infrastructure configuration not only extends the accessibility of wireless PCs to the wired LAN, but also doubles the effective wireless transmission range for wireless PCs by retransmitting incoming radio signals through the Wireless Barricade Plus.

A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, as shown in the following figure:

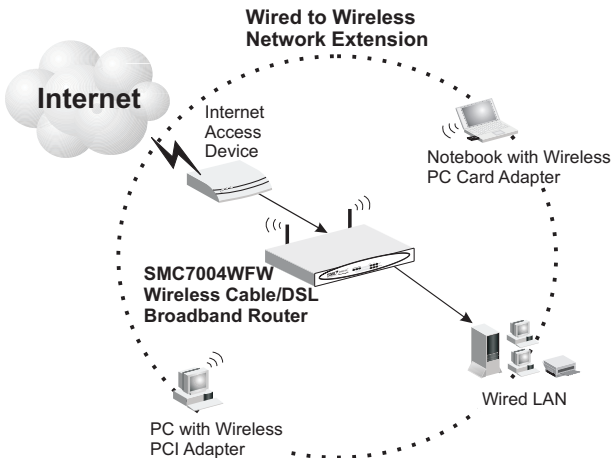


Figure 2-4. Making WLAN Connections

Attach the Wireless Barricade Plus to the Internet

If Internet services are provided through an xDSL or cable modem, use unshielded or shielded twisted-pair Ethernet cable (Category 3 or greater) with RJ-45 plugs to connect the broadband modem directly to the WAN port on the Wireless Barricade Plus. Use either straight through or crossover cabling depending on the port type provided by the modem (see Appendix B).

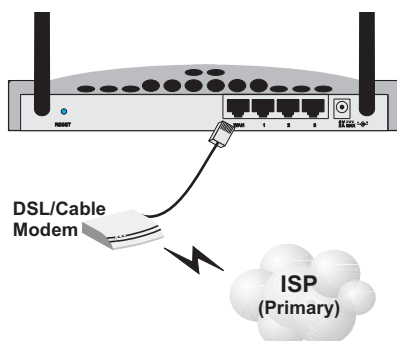


Figure 2-5. Making WAN Connection

Note: When connecting to the WAN port, use 100-ohm Category 3, 4 or 5 shielded or unshielded twisted-pair cable with RJ-45 connectors at both ends for all connections.

Connecting the Power Adapter

Plug the power adapter into the power socket on the Wireless Barricade Plus, and the other end into a power outlet. Check the indicator marked Power on the front panel to be sure it is on. If the Power indicator does not light up, refer to Troubleshooting in Appendix A.

Verify Port Status

Check the power and port indicators as shown in the following table.

LED	Condition	Status
Power (Green)	On	Wireless Barricade Plus is receiving power.
WLAN (Green)	On	The Wireless Barricade Plus has established a valid wireless connection.
WAN (Green)	On	The WAN port has established a valid network connection.
<i>LAN</i>		
Link (Green)	On	The indicated LAN port has established a valid network connection.
Activity (Amber)	Flashing	The indicated LAN port is transmitting or receiving traffic.

INSTALLATION

CHAPTER 3

CONFIGURING CLIENT PCs

TCP/IP Configuration

To access the Internet through the Barricade™ Plus Wireless Cable/DSL Broadband Router, you must configure the network settings of the computers on your LAN to use the same IP subnet as the Wireless Barricade Plus. The default network settings for the Wireless Barricade Plus are:

Gateway IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Note: These settings can be changed to fit your network requirements, but you must first configure at least one computer as described in Chapter 5 to access the Wireless Barricade Plus' Web configuration interface. (See Chapter 4 for information on configuring the Wireless Barricade Plus.)

If you have not previously configured TCP/IP for your computer, refer to “Installing TCP/IP Protocol in Your PC” on page 5-1.

All PCs connected to the Wireless Barricade Plus must be set to the same IP subnet as the Wireless Barricade Plus. The default subnet address of the Wireless Barricade Plus is 192.168.2.X (where X means 2–254) and the subnet mask is 255.255.255.0. You can set the IP address for client PCs either by automatically obtaining an IP address from the Wireless Barricade Plus' DHCP service or by manual configuration. See “Setting TCP/IP to Work with the Wireless Barricade Plus” on page 5-5.

TCP/IP CONFIGURATION

CHAPTER 4

CONFIGURING THE WIRELESS BARRICADE PLUS

After you have configured TCP/IP on a client computer, you can use a Web browser to configure the Barricade™ Plus Wireless Cable/DSL Broadband Router. The Wireless Barricade Plus can be configured by any Java-supported browser including Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above. Using the Web management interface, you can configure the Wireless Barricade Plus and view statistics to monitor network activity.

To access the Wireless Barricade Plus' management interface, enter the IP address of the Wireless Barricade Plus in your Web browser <http://192.168.2.1>. Then login the Wireless Barricade Plus system with no password (by default, there is no password).

Note: For some browsers it may be necessary to include “:88” after the management IP address. For example, <http://192.168.2.1:88>

The home page displays the “Setup Wizard” and “Advanced Setup” options.



Navigating the Web Browser Interface

The Wireless Barricade Plus’ management interface features a Setup Wizard and an Advanced Setup section. Use the Setup Wizard if you want to quickly setup the Wireless Barricade Plus for use with a cable modem or DSL modem.

Advanced setup supports more advanced functions like hacker attack detection, IP and MAC address filtering, intrusion detection, virtual server setup, virtual DMZ hosts, as well as other advanced functions.

Making Configuration Changes

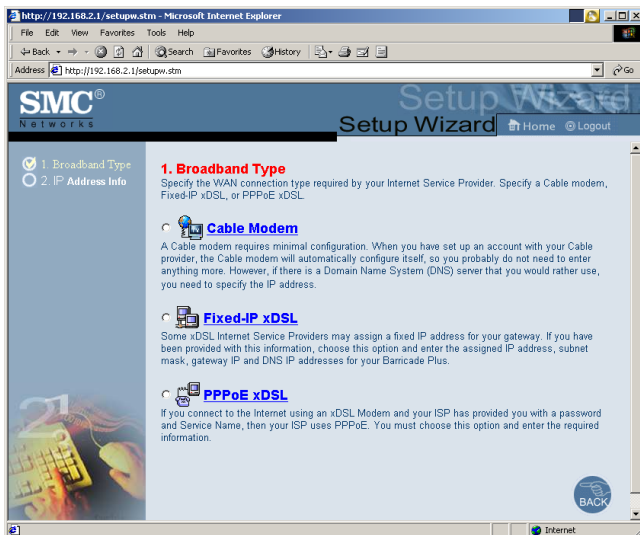
Configurable parameters have a dialog box. Once a configuration change has been made on a page, be sure to click the “Apply” or “Next” button at the bottom of the page to enable the new setting.

To ensure proper screen refresh after a command entry, be sure that Internet Explorer 5.0 is configured as follows: Under the menu “Tools/Internet Options/General/Temporary Internet Files/Settings,” the setting for “Check for newer versions of stored pages” should be “Every visit to the page.”

Setup Wizard

Broadband Type

Select the type of broadband connection you have.



Cable Modem

http://192.168.2.1/setupw.stm - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites History Print

Address http://192.168.2.1/setupw.stm Go

SMC[®] NETWORKS Setup Wizard Home Logout

1. Broadband Type
2. IP Address Info

2. IP Address Info

Cable Modem

Host Name

MAC Address

Release Renew

BACK HELP FINISH

Done Internet

Your ISP may have given you a host name. If so, enter it into this field.

Click “Finish” to complete the setup. The Status page will open to allow you to view the connection status, as well as other information. See “Status” on page 4-50 for details.

Fixed-IP xDSL

SMC® Networks Setup Wizard

Home Logout

1. Broadband Type
2. IP Address Info

2. IP Address Info

Fixed-IP xDSL

IP	0	0	0	0
Gateway IP	0	0	0	0
DNS	0	0	0	0
Subnet Mask	0	0	0	0

Enter the IP address, subnet mask, and gateway provided to you by your ISP in the appropriate fields.

BACK HELP FINISH

Done Internet

Some xDSL Internet Service Providers may assign a fixed (static) IP address for your gateway. If you have been provided with this information, choose this option and enter the assigned IP address, subnet mask, gateway IP, and DNS IP addresses for the Wireless Barricade Plus.

Click “Finish” to complete the setup. The Status page will open to allow you to view the connection status, as well as other information. See “Status” on page 4-50 for details.

PPPoE

The screenshot shows a web browser window titled "http://192.168.2.1/setupw.stm - Microsoft Internet Explorer". The address bar shows "http://192.168.2.1/setupw.stm". The page header includes the SMC Networks logo and the title "Setup Wizard" with links for "Home" and "Logout". On the left, a sidebar lists two steps: "1. Broadband Type" and "2. IP Address Info", with the second step being the active one. The main content area is titled "2. IP Address Info" and "PPPoE". It contains a form titled "Use PPPoE Authentication" with the following fields: "User Name", "Password", "Please retype your password", "Service Name", "MTU" (set to 1454 with a note "(1440 <= MTU Value <= 1492)"), and "Maximum Idle Time" (set to 10). There is a checked checkbox for "Auto-reconnect". At the bottom of the form, a note states: "Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a Service Name* enter it in the Service Name field, otherwise, leave it blank." At the bottom right of the form are three buttons: "BACK", "HELP", and "FINISH". The browser's status bar at the bottom shows "javascript:history.go(-1);" and "Internet".

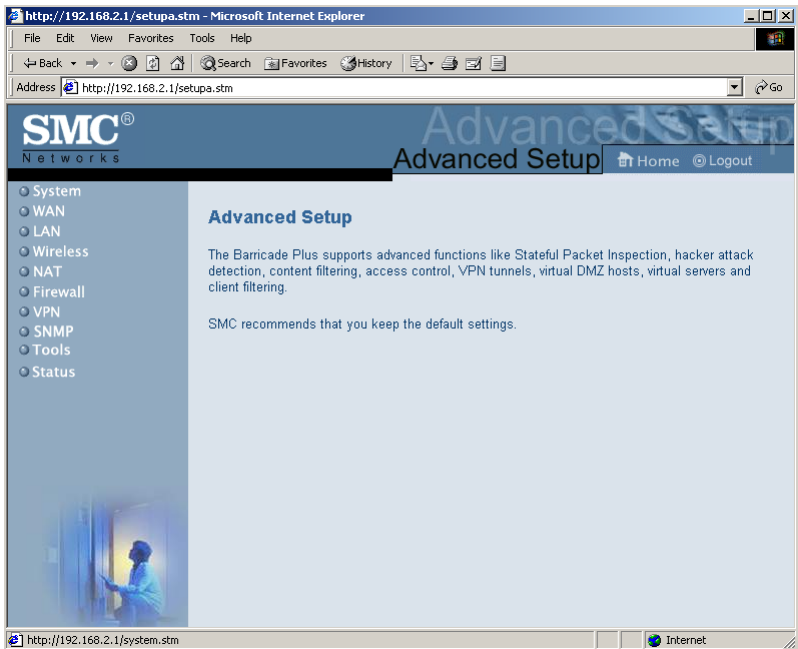
Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers.

Leave the Maximum Transmission Unit (MTU) on the default value (1492) unless you have a particular reason to change it.

Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, it will be dropped. Enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.

Advanced Setup Menu

Selecting the “Advanced Setup” displays the main menu on the left-hand side of the screen and descriptive information on the right-hand side. The Main Menu links are used to navigate to other menus that display configuration parameters and statistics.



Navigating the Web Browser Interface

The Wireless Barricade Plus’ advanced management interface includes ten key menus – System, WAN, LAN, Wireless, NAT, Firewall, VPN, SNMP, Tools, and Status. The System menu provides general information on the current settings and how to configure the Wireless Barricade Plus. The WAN, LAN, Wireless, NAT, Firewall, VPN and SNMP menus are used to configure the LAN, WAN and wireless interface, as well as other functions.

While the Tools menu is used to backup the Wireless Barricade Plus, restore the factory settings, update the firmware, or reset the Wireless Barricade Plus. The Status menu is used to see the connection status for the Wireless Barricade Plus' WAN/LAN interfaces, firmware, and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected on your network.

Main Menu

Using the Web management interface, you can define system parameters, manage and control the Wireless Barricade Plus and its ports, or monitor network conditions. The following table briefly describes the selections available from this "Advanced Setup" screen.

Menu	Description
<i>System Menu</i>	Configures TCP/IP settings and client services.
Time Zone	Sets the local time zone.
Password Settings	Sets the password for administrator access.
Remote Management	Sets the IP address for remote management station.
<i>WAN Menu</i>	• Specifies the Internet connection type: (1) Dynamic IP host configuration and the physical MAC address of each media interface, (2) PPPoE configuration, or (3) Static IP and gateway address. • Specifies DNS servers to use for domain name resolution.
<i>LAN Menu</i>	Sets the TCP/IP configuration of the Wireless Barricade Plus' LAN interface and all DHCP clients.
<i>Wireless</i>	Configures the radio frequency, SSID, and encryption for wireless communications.
<i>NAT Menu</i>	Configures system IP settings, including: • Address Mapping • Virtual Server

Menu	Description
<i>Firewall Menu</i>	Configures a variety of packet filtering and specialized functions, including: • Access Control • URL Blocking • Schedule Rule • Intusion Detection • DMZ (Demilitarized Zone)
<i>VPN Menu</i>	Provides Virtual Private Network tunneling capability for secure Internet communication.
IPsec	Configures inbound Security Association (SA).
PPTP	• Authorizes remote users using the PPTP tunneling protocol. • Authenticates a PPTP tunnel to the destination host and authorizes the IP address range to assign to the client users.
<i>SNMP Menu</i>	Displays and modifies parameters for the Simple Network Management Protocol (SNMP).
Community	Configures the community strings authorized for management access. Up to 5 community names may be entered.
Trap	Specify management stations that will receive authentication failure messages or other unsolicited message from the SNMP agent. Up to 5 trap managers may be entered.
<i>Tools Menu</i>	Contains options to reset the system, restore configuration settings, or update system firmware.
Configuration Tools	Allows you to backup the system configurations, restore the saved backup configuration file, or restore all configuration settings to the factory defaults.
Firmware Upgrade	Upgrades the system with the latest firmware obtained from SMC's website at www.smc.com
Reset	Reboots the system and retains all of your configuration settings.

Menu	Description
<i>Status Menu</i>	Displays WAN/LAN connection status, firmware and hardware version numbers, as well as information on all DHCP client PCs connected.
<i>Help Button</i> 	Contains information for product support, troubleshooting, and network terminology.
<i>Home Button</i> 	Go to the overview page of this Web management interface.
<i>Logout Button</i> 	Exit the Wireless Barricade Plus system.

Making Configuration Changes

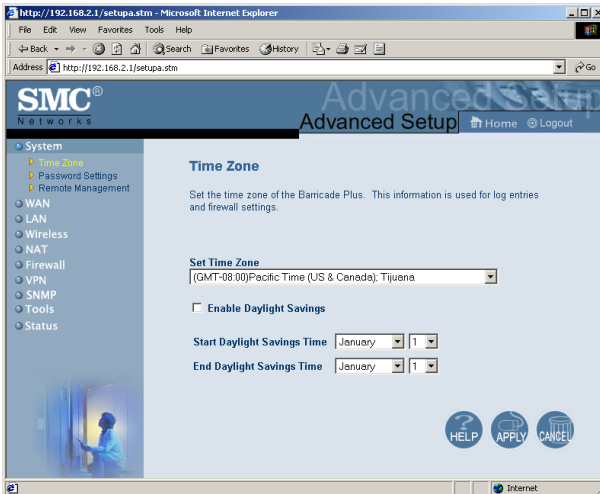
Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click the “**APPLY**” button at the bottom of the page to confirm the new settings.



Note: To ensure proper screen refresh after a command entry, be sure that Internet Explorer 5.0 is configured as follows: Under the menu “Tools/Internet Options/General/Temporary Internet Files/Settings,” the setting for “Check for newer versions of stored pages” should be “Every visit to the page.”

System Settings

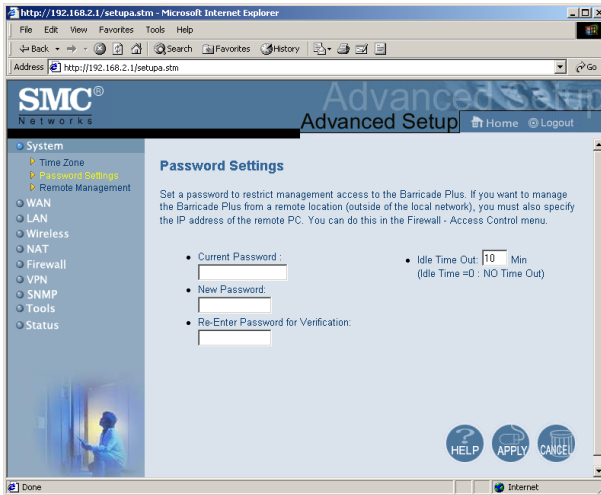
Set Time Zone



Set the time zone for the Wireless Barricade Plus. This information is used for log entries and client filtering.

Setting a Password

If this is your first time to access the Wireless Barricade Plus, you should define a new password, record it and put it in a safe place. From the “Advanced Setup” menu, select “System” and click on “Password Settings” and follow the instructions on the screen.

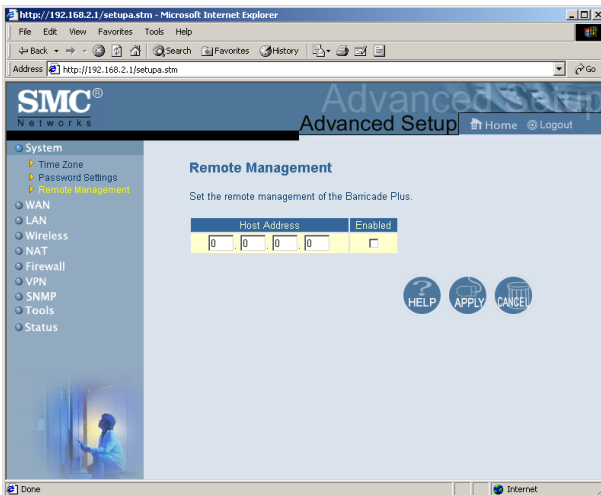


Use this menu to restrict management access based on a specific password. Anyone can access the “Setup Wizard,” “Advanced Setup” and Help menus, but you must enter a password to access the configuration options provided by the “Setup Wizard” and “Advanced Setup” menus. By default, there is no password. Please assign a password to the Wireless Barricade Plus as soon as possible, and store it in a safe place.

Passwords can contain from 3–12 alphanumeric characters, and are case sensitive.

Note: If your password is lost, or you cannot gain access to the management interface, press the Reset button on the front panel (holding it down for at least five seconds) to restore the factory defaults.

Remote Management



By default, management access is only available to users on your local network. However, you can also manage the Wireless Barricade Plus from a remote host by adding the IP address of an administrator to this screen.

Note: If you specify an IP address of 0.0.0.0, any host can manage the Wireless Barricade Plus. You can also manage the Wireless Barricade Plus from a remote host by typing “http://192.168.2.1:8080” in the “Address” field of your Web browser.

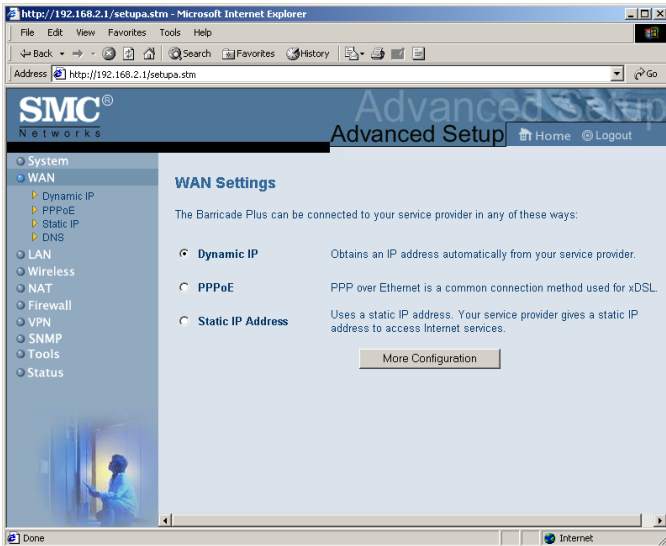
Networking and Client Services

You can use the “Setup Wizard” to change the required settings, or you can select the basic configuration items you need to change from the “Setup Wizard” screen.

Use the “Advanced Setup” menu to configure the WAN connection options, the LAN interface (including TCP/IP parameters for the Wireless Barricade Plus’ gateway address, DHCP address pool for dynamic client address allocation), and other advanced services.

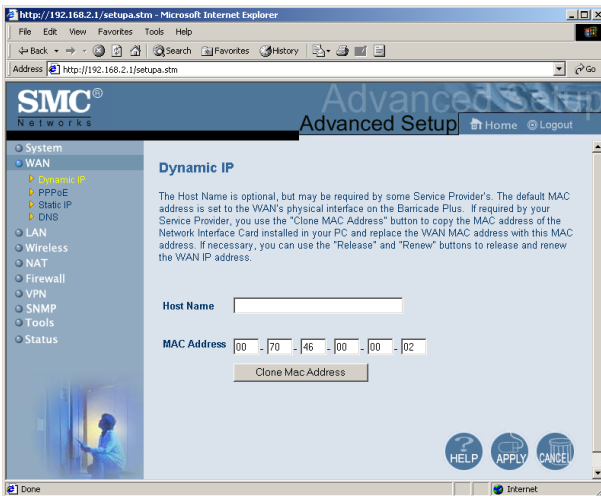
WAN Configuration

Specify the WAN connection type required by your Internet Service Provider, then click “More Configuration” to provide detailed configuration parameters for the selected connection type.



Specify one of the first three options to configure a WAN connection through the RJ-45 port (i.e., a connection to an xDSL modem or cable modem).

Dynamic IP Address – DHCP



The Host Name is optional, but may be required by some ISPs.

The default MAC address is set to the WAN's physical interface on the Wireless Barricade Plus. Use this address when registering for Internet service, and do not change it unless required by your ISP.

PPP over Ethernet – PPPoE

The screenshot shows a web browser window displaying the SMC Advanced Setup interface. The left sidebar contains a navigation menu with options: System, WAN, Dynamic IP, Static IP, DNS, LAN, Wireless, NAT, Firewall, VPN, SNMP, Tools, and Status. The main content area is titled 'PPPoE' and contains the following text: 'Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.' Below this text, it says 'If your Internet Service Provider requires the use of PPPoE, enter the information below.' A form titled 'Use PPPoE Authentication' contains the following fields: 'User Name', 'Password', 'Please retype your password', 'Service Name', 'MTU' (with a value of 1454 and a note '(1440 <= MTU Value <= 1492)'), 'Maximum Idle Time' (with a value of 10), and a checked 'Auto-reconnect' checkbox. At the bottom of the browser window, there are buttons for 'HELP', 'APPLY', and 'CANCEL', and a status bar showing 'Done' and 'Internet'.

http://192.168.2.1/setupa.htm - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites History

Address http://192.168.2.1/setupa.htm

SMC® Advanced Setup

Home Logout

System

WAN

Dynamic IP

Static IP

DNS

LAN

Wireless

NAT

Firewall

VPN

SNMP

Tools

Status

PPPoE

Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.

If your Internet Service Provider requires the use of PPPoE, enter the information below.

Use PPPoE Authentication

User Name :

Password :

Please retype your password :

Service Name :

MTU : (1440 <= MTU Value <= 1492)

Maximum Idle Time

☒ Auto-reconnect

Done

HELP APPLY CANCEL

Internet

Enter the PPPoE user name and password by your ISP.
The Service Name is normally optional, but may be required by some providers.

Specify the value of MTU (Maximum Transmission Unit) for proper Internet access such as browsing web sites and using E-mail.
(Default: 1492)

Enter the maximum idle time for the Wireless Barricade Plus (in seconds).

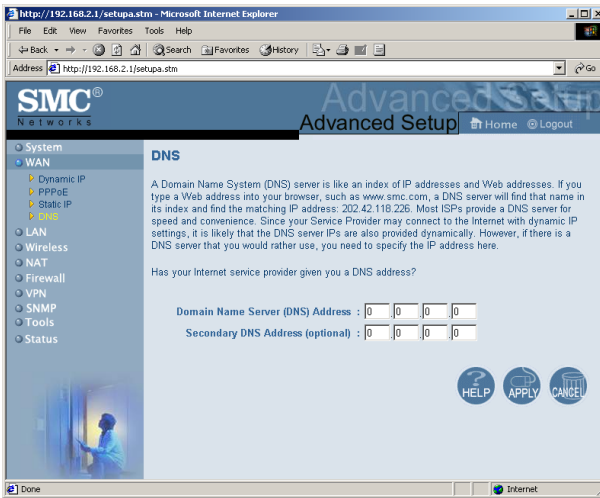
Static IP Address – Fixed IP

The screenshot shows a web browser window titled "Microsoft Internet Explorer" with the address bar displaying "http://192.168.2.1/setupa.htm". The page header includes the "SMC Networks" logo and the title "Advanced Setup". A left-hand navigation menu lists various system settings: System, WAN, Dynamic IP, PPPoE, Static IP (highlighted), DNS, LAN, Wireless, NAT, Firewall, VPN, SNMP, Tools, and Status. The main content area is titled "Static IP" and contains the following text: "If your Service Provider has assigned a fixed IP address, enter the assigned IP address, subnet mask and the gateway address provided." Below this, a question asks: "Has your Service Provider given you an IP address and Gateway address?". Three input fields are provided for "IP address assigned by your Service Provider", "Subnet Mask", and "Service Provider Gateway Address", each with a numeric keypad interface. At the bottom right, there are three buttons: "HELP", "APPLY", and "CANCEL".

If your Internet Service Provider has assigned a fixed address, enter the assigned address and subnet mask for the Wireless Barricade Plus, then enter the gateway address of your ISP.

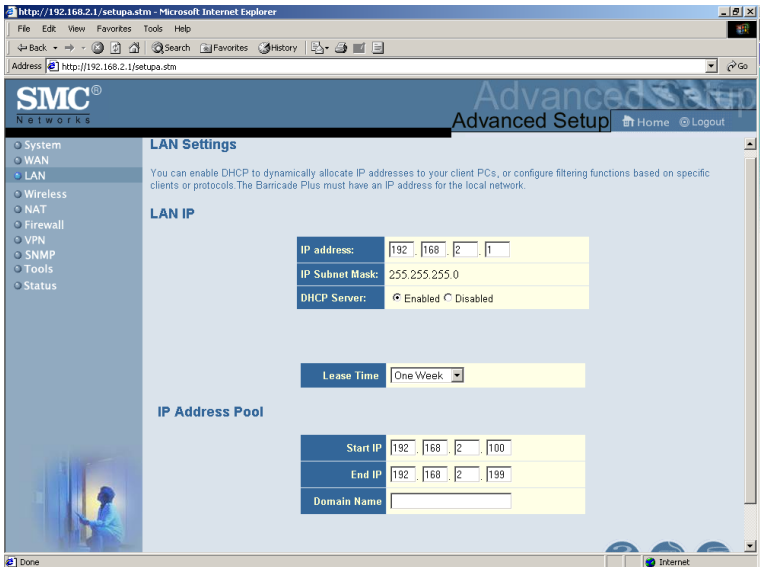
Note: You may need a fixed address if you want to provide Internet services, such as a Web server or FTP server.

DNS Configuration



Domain Name Servers are used to map an IP address to the equivalent domain name (e.g., www.smc.com). Your ISP should provide the IP address for one or more domain name servers. Enter those addresses on this screen.

LAN Gateway and DHCP Settings



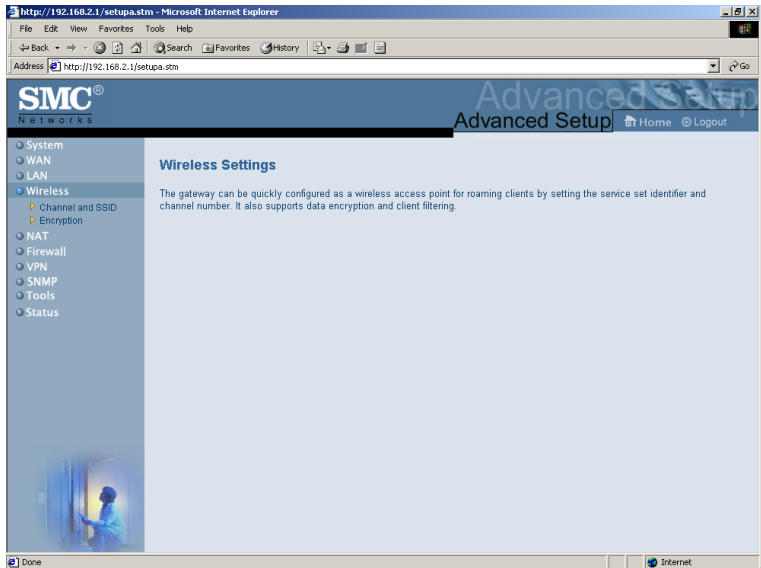
Configure the gateway address of the Wireless Barricade Plus. To dynamically assign the IP address for client PCs, enable the DHCP Server, set the lease time, and then specify the address range. Also remember to configure all of your client PCs for dynamic address allocation.

Valid IP addresses consist of four numbers, and are separated by periods. The first three fields are the network portion, and can be from 0–255, while the last field is the host portion and can be from 1–254. However, remember not to include the gateway address of the Wireless Barricade Plus in the client address pool. If you change the pool range, make sure the first three octets match the gateway’s IP address, i.e., 192.168.2.xxx.

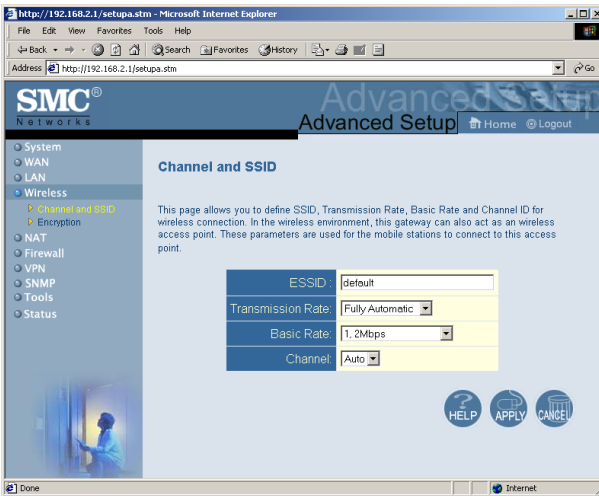
Note: Verify that your IP address pool is from 192.168.2.2 to 192.168.2.254, your subnet mask is 255.255.255.0 and your default gateway is 192.168.2.1.

Wireless Configuration

To configure the Wireless Barricade Plus as a wireless access point for wireless clients (either stationary or roaming), all you need to do is define the radio channel, the Service Set identifier (SSID), and encryption options.



Channel and SSID

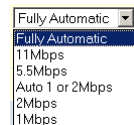


You must specify a common radio channel and SSID (Service Set ID) to be used by the Wireless Barricade Plus and all of your wireless clients. Be sure you configure all of your clients to the same values.

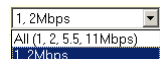
ESSID: The Service Set ID. This should be set to the same value as other wireless devices in your network.

Note: The SSID is case sensitive and can consist of up to 32 alphanumeric characters.

Transmission Rate: Set the data rate transmitted from the Wireless Barricade Plus. The lower the data rate, the longer the transmission distance. (Default: Fully Automatic)



Basic Rate: Select “All (1, 2, 5.5, 11Mbps)” from the drop-down list to optimize the data transfer speed for your network. (Default: 1, 2Mbps)



Channel: The radio channel through which the Wireless Barricade Plus communicates to PCs in its BSS. (Default: “Auto”)

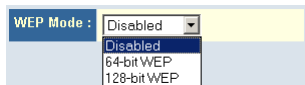


Note: The available channel settings are limited to local regulations, which determine the number of channels that are available.

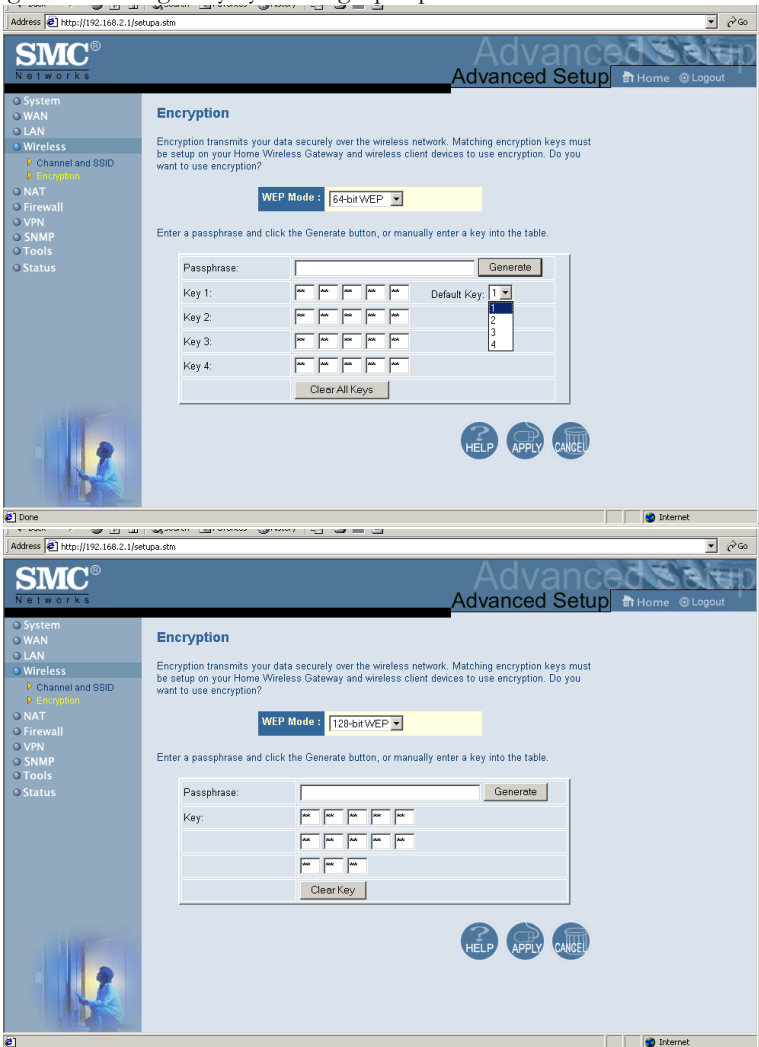
Encryption



If you are transmitting sensitive data across wireless channels, you should enable Wired Equivalent Privacy (WEP) encryption. Encryption requires you to use the same set of encryption/decryption keys for the Wireless Barricade Plus and all of your wireless clients. You can choose between standard 64-bit or the more robust 128-bit encryption keys.



You can automatically generate encryption keys or you can manually enter the keys. For automatic 64-bit security, you enter a passphrase that is used to create four keys (as shown below). The automatic 128-bit security generates a single key by entering a passphrase.

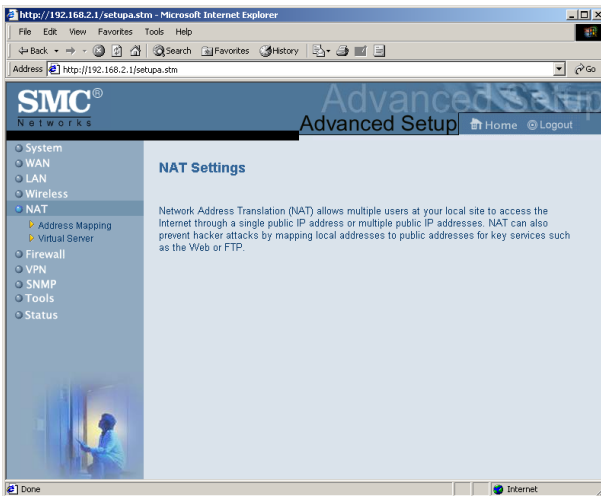


If you use encryption, configure the same keys used for the Wireless Barricade Plus on each of your wireless clients. Note that the Wired Equivalent Privacy (WEP) protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

Configuring Client Services

The Wireless Barricade Plus includes a broad range of client services, including firewall protection, VPN tunneling capability, network address translation, virtual server, address mapping, DMZ, and restricted Internet access for specified clients. You can configure these functions by selecting specific items from the menu on the left of the screen.

NAT - Network Address Translation



Network Address Translation (NAT) provides multiple Internet connections using single IP address. If you need multiple connections, use the following screen to specify the public IP addresses to be opened for your client users. NAT can also prevent hacker attacks by mapping local addresses to public addresses for key services such as the Web or FTP.

Address Mapping

SMC[®] Networks Advanced Setup | Home | Logout

Address Mapping

Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This feature limits the number of public IP addresses required from the ISP and also maintains the privacy and security of the local network. We allow one or more than one public IP address to be mapped to a pool of local addresses.

Address Mapping	
1. Global IP: 0.0.0.0 is transformed as multiple virtual IPs	from 192.168.2.0 to 192.168.2.0
2. Global IP: 0.0.0.0 is transformed as multiple virtual IPs	from 192.168.2.0 to 192.168.2.0
3. Global IP: 0.0.0.0 is transformed as multiple virtual IPs	from 192.168.2.0 to 192.168.2.0
4. Global IP: 0.0.0.0 is transformed as multiple virtual IPs	from 192.168.2.0 to 192.168.2.0
5. Global IP: 0.0.0.0 is transformed as multiple virtual IPs	from 192.168.2.0 to 192.168.2.0
6. Global IP: 0.0.0.0 is transformed as multiple virtual IPs	from 192.168.2.0 to 192.168.2.0
7. Global IP: 0.0.0.0 is transformed as multiple virtual IPs	from 192.168.2.0 to 192.168.2.0
8. Global IP: 0.0.0.0 is transformed as multiple virtual IPs	from 192.168.2.0 to 192.168.2.0
9. Global IP: 0.0.0.0 is transformed as multiple virtual IPs	from 192.168.2.0 to 192.168.2.0
10. Global IP: 0.0.0.0 is transformed as multiple virtual IPs	from 192.168.2.0 to 192.168.2.0

HELP APPLY CANCEL

Use the “Address Mapping” option to limit the number of public IP addresses required from the ISP and maintain the privacy and security of the local network.

CONFIGURING THE WIRELESS BARRICADE PLUS

Virtual Server

https://192.168.2.1/setupa.htm - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.2.1/setupa.htm

SMC® Advanced Setup Home Logout

System
WAN
LAN
Wireless
NAT
Address Mapping
Virtual Server
Firewall
VPN
SNMP
Tools
Status

Virtual Server

You can configure the Barricade Plus as a virtual server, so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP) port number, the Barricade Plus redirects the external service request to the appropriate server (located at another internal IP address).

	Private IP	Private Port	Type	Public Port
1.	192.168.2. 		TCP UDP	
2.	192.168.2. 		TCP UDP	
3.	192.168.2. 		TCP UDP	
4.	192.168.2. 		TCP UDP	
5.	192.168.2. 		TCP UDP	
6.	192.168.2. 		TCP UDP	
7.	192.168.2. 		TCP UDP	
8.	192.168.2. 		TCP UDP	
9.	192.168.2. 		TCP UDP	
10.	192.168.2. 		TCP UDP	
11.	192.168.2. 		TCP UDP	
12.	192.168.2. 		TCP UDP	
13.	192.168.2. 		TCP UDP	
14.	192.168.2. 		TCP UDP	
15.	192.168.2. 		TCP UDP	
16.	192.168.2. 		TCP UDP	
17.	192.168.2. 		TCP UDP	
18.	192.168.2. 		TCP UDP	
19.	192.168.2. 		TCP UDP	
20.	192.168.2. 		TCP UDP	

HELP APPLY CANCEL

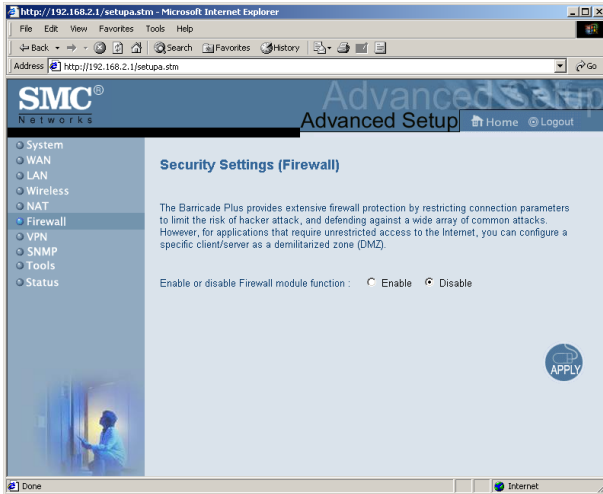
If you configure the Wireless Barricade Plus as a virtual server, remote users accessing services such as Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the Wireless Barricade Plus redirects the external service request to the appropriate server (located at another internal IP address).

The WAN interface must have a fixed IP address to utilize this function. For example, if you set Type/Public Port to TCP/80 (HTTP or Web) and the Private IP/Port to 192.168.2.2/80, then all HTTP request from outside users will be transferred to 192.168.2.2. Therefore, by just entering the IP Address provided by the ISP, Internet users can access the service they need at the local address to which you redirect them.

Some of the more common TCP service ports include:

HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

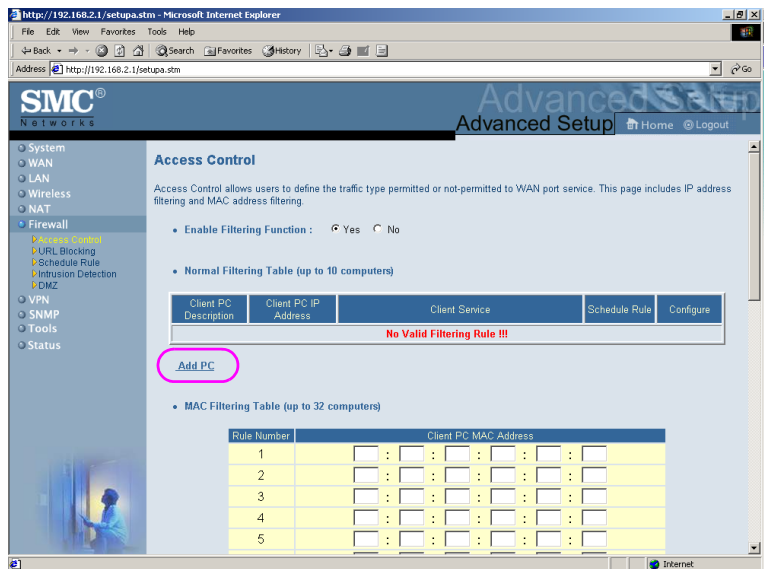
Firewall Protection



The Wireless Barricade Plus' firewall can provide the access control of connected client PCs, block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. The firewall does not significantly affect system performance, so we advise setting it enabled to protect your network users by selecting “Enable” on the screen.

Note: When you select the “Enable” radio button of the “Enable or disable Firewall module function” field, be sure to press the “APPLY” button.

Access Control



Using this option allows you to specify different privileges for the client PCs (up to 32 computers).

The following items are included in the “Access Control” screen:

Field	Description
Normal Filtering Table	Displays the IP address and filtering status of the connected client PC
MAC Filtering Table	Displays the MAC address of the client PC

Note: Click on “Add PC” and define the appropriate settings for client PC services (as shown in the following screen).

SMC Networks Advanced Setup

Home Logout

- System
 - WAN
 - LAN
 - Wireless
 - NAT
 - Firewall
 - Access Control
 - URL Blocking
 - Schedule Rule
 - Intrusion Detection
 - DMZ
 - VPN
 - SNMP
 - Tools
 - Status

Access Control Add PC

This page allows users to define service limitation of client PC, including IP address, service type and scheduling rule criteria. For URL blocking function, you need to configure URL address first in "URL Blocking" page. For scheduling function, you also need to configure schedule rule first in "Schedule Rule" page.

- Client PC Description:
- Client PC IP Address: 192.168.2. ~
- Client PC Service:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3120, 8000, 8080, 8081	☐
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	☐
E-mail Sending	SMTP, TCP Port 25	☐
News Forums	NNTP, TCP Port 119	☐
E-mail Receiving	POP3, TCP Port 110	☐
Secure HTTP	HTTPS, TCP Port 443	☐
File Transfer	FTP, TCP Port 21	☐
MSN Messenger	TCP Port 1863	☐
Telnet Service	TCP Port 23	☐
AIM	AOL Instant Messenger, TCP Port 5190	☐
NetMeeting	H.323, TCP Port 1720	☐
DNS	UDP Port 53	☐
SNMP	UDP Port 161, 162	☐
VPN-PPTP	TCP Port 1723	☐
VPN-L2TP	UDP Port 1701	☐
TCP	All TCP Port	☐
UDP	All UDP Port	☐

User Define Service

Protocol: ☐ TCP ☐ UDP

Port Range: ~ , ~ , ~ , ~ , ~

Scheduling Rule (Ref. Schedule Rule Page):

OK Cancel

URL Blocking

SMC®
Networks

Advanced Setup

Home Logout

System

WAN

LAN

Wireless

NAT

Firewall

Access Control

Schedule Rule

Intrusion Detection

DMZ

VPN

SNMP

Tools

Status

URL Blocking

Disallowed Web Sites and Keywords.

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.

To specify the particular PC, go back to the "Access Control" page and check the box for "Http with URL Blocking" in the "Normal Filtering Table".

Rule Number	URL / Keyword	Rule Number	URL / Keyword
Site 1		Site 16	
Site 2		Site 17	
Site 3		Site 18	
Site 4		Site 19	
Site 5		Site 20	
Site 6		Site 21	
Site 7		Site 22	
Site 8		Site 23	
Site 9		Site 24	
Site 10		Site 25	
Site 11		Site 26	
Site 12		Site 27	
Site 13		Site 28	
Site 14		Site 29	
Site 15		Site 30	

Clear All

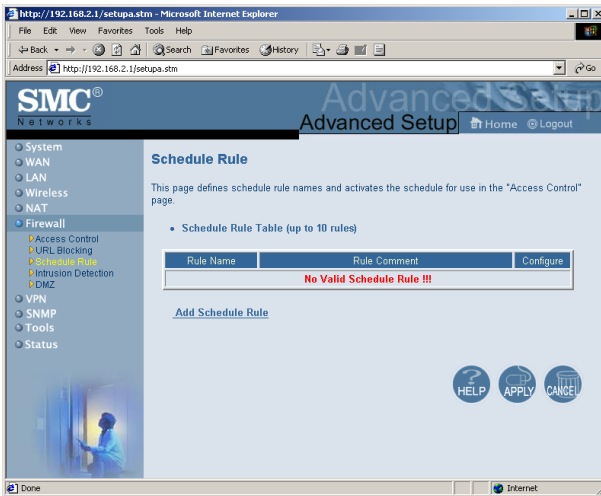
HELP

APPLY

CANCEL

Using the above screen to block access to the Web sites specified in the table.

Schedule Rule



You can filter Internet access for local clients based on the “Rule Name,” and time of day.

1. Click on “Add Schedule Rule”
2. Define the appropriate settings for a schedule rule (as shown in the following screen).
3. Click “OK” and then the “APPLY” button to save your settings. (as shown on previous page)

The screenshot shows a web browser window with the address `http://192.168.2.1/setupa.stm`. The page title is "SMC Networks Advanced Setup". On the left is a navigation menu with the following items: System, WAN, LAN, Wireless, NAT, Firewall (selected), Access Control, URL Blocking, Intrusion Detection, DMZ, VPN, SNMP, Tools, and Status. The main content area is titled "Edit Schedule Rule". It contains two text input fields: "Name:" and "Comment:". Below these is a section labeled "Activate Time Period:" which contains a table with three columns: "Week Day", "Start Time (hh:mm)", and "End Time (hh:mm)". The table has seven rows for the days of the week. Each cell in the "Start Time" and "End Time" columns contains two input boxes for hours and minutes. At the bottom of the table are "OK" and "Cancel" buttons. The browser's status bar at the bottom shows "Done" and "Internet".

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	:	:
Sunday	:	:
Monday	:	:
Tuesday	:	:
Wednesday	:	:
Thursday	:	:
Friday	:	:
Saturday	:	:

Intrusion Detection

http://192.168.2.1/setupa.htm - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.2.1/setupa.htm

SMC® **Advanced Setup** Home Logout

System
WAN
LAN
Wireless
NAT
Firewall
Access Control
URL Blocking
Schedule Rule
Intrusion Detection
DMZ
VPN
SNMP
Tools
Status

Intrusion Detection

When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the Barricade Plus will support full operation as initiated from the local LAN.

The Barricade Plus firewall can block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, TCP null scan, and TCP SYN flooding.

- Intrusion Detection Feature**

SPI and Anti-DOS firewall protection :	☒
RIP detect :	☒
Discard Ping From WAN :	☐
- Stateful Packet Inspection**

Packet Fragmentation	☒
TCP Connection	☒
UDP Session	☒
FTP Service	☒
H.323 Service	☒
TFTP Service	☒
- When hackers attempt to enter your network, we can alert you by e-mail**

Your E-mail Address :

SMTP Server Address :

POP3 Server Address :

User name :

Password :
- Connection Policy**

Fragmentation half-open wait: 10 sec

TCP SYN wait: 30 sec

TCP FIN wait: 5 sec

TCP connection idle timeout: 3600 sec

UDP session idle timeout: 30 sec

H.323 data channel idle timeout: 180 sec
- DoS Detect Criteria:**

Total incomplete TCP/UDP sessions HIGH: 300 session

Total incomplete TCP/UDP sessions LOW: 250 session

Incomplete TCP/UDP sessions (per min) HIGH: 250 session

Incomplete TCP/UDP sessions (per min) LOW: 200 session

Maximum incomplete TCP/UDP sessions number from same host: 10

Incomplete TCP/UDP sessions detect sensitive time period: 300 msec

Maximum half-open fragmentation packet number from same host: 30

Half-open fragmentation detect sensitive time period: 10000 msec

Flooding cracker block time: 300 sec

HELP APPLY CANCEL

The Intrusion Detection feature of the Wireless Barricade Plus limits the access of the incoming traffic from the WAN port. When the SPI feature is turned on, all the incoming packets will be blocked unless certain types of traffic types are checked by the users. When the user checks certain types of traffic, only the particular type of traffic initiated from the Internal LAN will be allowed. For example, if the user only checks “FTP service” from the Stateful Packet Inspection heading, all the incoming traffic will be blocked except the FTP connection initiated from the local LAN.

- *Stateful Packet Inspection*

This option allows you to select different application types that are using dynamic port numbers. If you need to use the Stateful Packet Inspection (SPI) for blocking packets, check the radio button in the “Enable SPI and Anti-DoS firewall protection” field and then check the inspection type that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service, H.323 Service and TFTP Service.

- *Hacker Prevention Feature*

The Wireless Barricade Plus’ firewall inspects packets at the application layer, and maintains TCP and UDP session information, including timeouts and number of active sessions, provides the ability to detect and prevent certain types of network attacks such as DoS attacks.

Network attacks that deny access to a network device are called denial-of-service (DoS) attacks. Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resource.

By using the above inspected information and timeout/threshold criteria, the Wireless Barricade Plus provides the following DoS attack preventions: Ping of Death (Ping flood) attack, SYN flood attack, IP fragment attack (Teardrop Attack), Brute-force attack, Land Attack, IP Spoofing attack, IP with zero length, TCP null scan (Port Scan Attack), UDP port loopback, Snork Attack etc..

Note: The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network users.

- *When hackers attempt to enter your network, we can alert you by e-mail*

Enter your E-mail address for alerting hacker access.

Specify your E-mail servers, user name and password.

- *Connection Policy*

Enter the appropriate values for TCP/UDP sessions

- *DoS Criteria and Port Scan Criteria*

Setup DoS and port scan criteria in the spaces provided.

DMZ (Demilitarized Zone)

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with options: System, WAN, LAN, Wireless, NAT, Firewall (selected), DMZ, VPN, SNMP, Tools, and Status. The Firewall menu is expanded, showing sub-options: Access Control, URL Blocking, Schedule Rule, Stateful Packet Inspection, and Hacker Prevention. The DMZ option is highlighted in yellow. The main content area is titled 'DMZ(Demilitarized Zone)' and contains the following text: 'If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.' Below this is a section 'Enable DMZ:' with radio buttons for 'Yes' (selected) and 'No'. A paragraph follows: 'Multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To use the DMZ, you must set a static IP address for that PC.' There are two columns of IP address input fields. The first column is labeled 'Public IP Address' and contains a list starting with '1. 10.2.12.96' followed by eight empty fields. The second column is labeled 'Client PC IP Address' and contains eight fields, each pre-filled with '192.168.2.0'. At the bottom right are three buttons: HELP, APPLY, and CANCEL.

SMC[®]
Networks

Advanced Setup
Home Logout

System
WAN
LAN
Wireless
NAT
Firewall
DMZ
VPN
SNMP
Tools
Status

Access Control
URL Blocking
Schedule Rule
Stateful Packet Inspection
Hacker Prevention

DMZ(Demilitarized Zone)

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.

Enable DMZ: ☒ Yes ☐ No

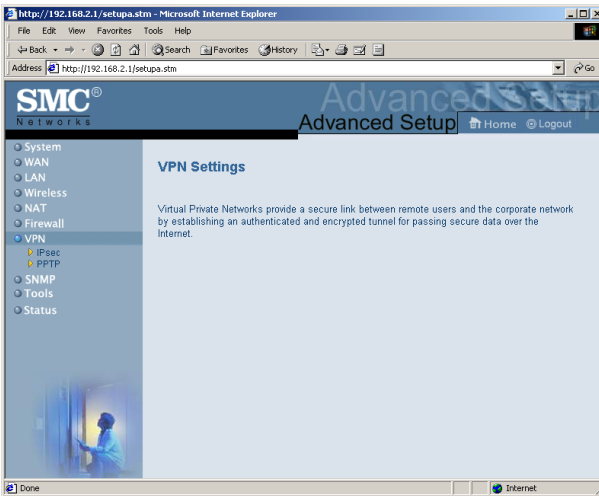
Multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To use the DMZ, you must set a static IP address for that PC.

Public IP Address	Client PC IP Address
1. 10.2.12.96	192.168.2.0
2. [0][0][0][0]	192.168.2.0
3. [0][0][0][0]	192.168.2.0
4. [0][0][0][0]	192.168.2.0
5. [0][0][0][0]	192.168.2.0
6. [0][0][0][0]	192.168.2.0
7. [0][0][0][0]	192.168.2.0
8. [0][0][0][0]	192.168.2.0

HELP APPLY CANCEL

If you have a client PC that cannot run an Internet application properly from behind the firewall, then you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ host to this screen. Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks, so only use this option as a last resort.

Virtual Private Networks (VPN) Tunnel



VPN provides a flexible and secure network to the authenticate users through IPsec (IP Security) and PPTP (Point-to-Point Tunneling Protocol) sessions.

IPsec

IPsec is a set of protocols that offers more secure security services in the extranet VPNs.

On the IPsec screen, select “Yes” in the “Enable IPsec” field for using the IPsec service, and choose the appropriate tunnel (Tunnel 1 - 3) as required.

Then you have to define the authentication algorithms of the Security Association (SA) by entering appropriate values in the “Inbound SA” and “Outbound SA” fields for using IPsec security control.

Notes: 1. Be sure the two sides of the VPN tunnel have the same security information.

2. Provide the “Remote IP Address” to remotely log on the network.

The screenshot shows a web browser window titled "http://192.168.2.1/setupa.stm - Microsoft Internet Explorer". The address bar shows "http://192.168.2.1/setupa.stm". The page is titled "SMC® Advanced Setup" with a navigation bar containing "Home" and "Logout". A left sidebar lists various system settings: System, WAN, LAN, Wireless, NAT, Firewall, VPN (selected), IPSec, PPTP, SNMP, Tools, and Status. The main content area is titled "IPsec" and includes a description: "IPsec allows users to define three secure IPsec tunnels with remote end points. This page includes the setting for both ends of each secure tunnel and the inbound/outbound Security Association (SA).". The configuration fields are as follows:

- Enable IPsec:** ☒ Yes ☐ No
- Tunnel:** Tunnel 1 (dropdown menu)
- Tunnel Enable :** ☐ Yes ☒ No
- Inbound SA** (same as Outbound SA)
 - SPI:** 256
 - Local IP Address:** 192.168.2.0 (IP address field)
 - Subnet Mask:** 255.255.255.0 (Subnet mask field)
 - Remote IP Address:** 192.168.3.0 (IP address field)
 - Subnet Mask:** 255.255.255.0 (Subnet mask field)
 - Security Gateway:** 192.168.1.100 (IP address field)
 - Hash Algorithm:** ☐ None ☒ MD5(32 character) ☐ SHA1(40 character)
 - Key:** 123456789abcdef02468ace013579bdc
 - Encrypt Algorithm:** ☐ None ☒ 3DES_CBC(48 character) ☐ DES_CBC(16 character)
 - Key:** 0123456789abcdef02468ace13579bdc

At the bottom right, there are three buttons: HELP, APPLY, and CANCEL. The browser status bar at the bottom shows "Done" and "Internet".

PPTP

Point-to-Point Tunneling Protocol (PPTP) allows the secure remote access over the Internet by simply dialing in a local point provided by an ISP. The following screen display the account information of the authorized remote users and the IP address range to assign to those users

SMC® Networks Advanced Setup | Home | Logout

- System
- WAN
- LAN
- Wireless
- NAT
- Firewall
- VPN
 - IPsec
 - PPTP**
- SNMP
- Tools
- Status

PPTP

The Barricade Plus allows PCs from the Internet to remotely log into the LAN using the PPTP tunneling protocol. This page includes the user name and password for the remote users who are authorized to log into the local LAN and the IP address range to assign to those users.

Index	Description	Accept to connect
1	user=Jason, pptp client, auto reconnect	Edit Clear ☐
2		Edit Clear ☐
3		Edit Clear ☐
4		Edit Clear ☐
5		Edit Clear ☐
6		Edit Clear ☐
7		Edit Clear ☐
8		Edit Clear ☐
9		Edit Clear ☐
10		Edit Clear ☐
11		Edit Clear ☐
12		Edit Clear ☐
13		Edit Clear ☐
14		Edit Clear ☐
15		Edit Clear ☐
16		Edit Clear ☐
17		Edit Clear ☐
18		Edit Clear ☐
19		Edit Clear ☐
20		Edit Clear ☐

IP Address Pool:

Start address:	192	168	4	100
End address:	192	168	4	110

HELP APPLY CANCEL

Click “Edit” on the screen to setup a PPTP session.

PPTP Tunnel Setting

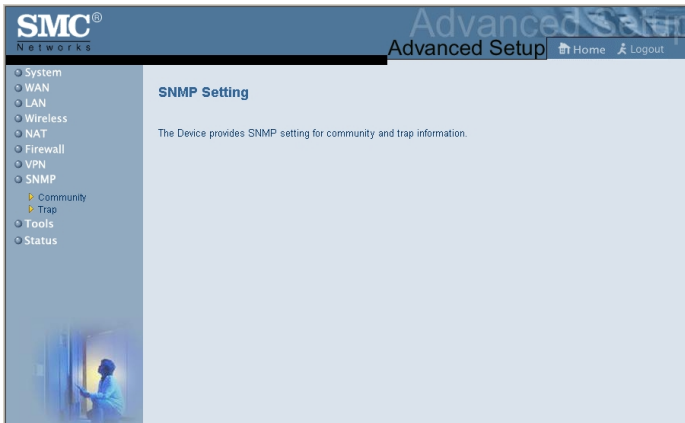
This page contains the detail PPTP tunnel settings. You may specify the Idle Time Out which defines the idle time out period when PPP session will be terminated after the period of time without traffic going through. You may also configure the tunnel to behave as either client or server. No more than one PPTP client is allowed to be enabled at any time. For a client tunnel, both host mode and router mode (LAN-to-LAN) are supported. The tunnel can also be configured to automatically reconnect to the server when there is Internet traffic generated.

User name:	Jason			
password:	*****			
Idle Time Out:	10 (Min)			
IP:	192	168	2	101
Subnet Mask:	255	255	255	0
Gateway IP:	192	168	2	1
Client Setting:	☒ pptp client ☒ host ☒ auto reconnect			

Using the above screen allows client PCs to establish a normal PPTP session and provides hassle-free configuration of the PPTP client on each client PC.

SNMP

Use the SNMP configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the agent are controlled by community strings. To communicate with the Wireless Barricade Plus, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following sections.



Community

The screenshot shows the 'SNMP Community' configuration window in the SMC Networks Advanced Setup application. The left sidebar contains a tree view with options: System, WAN, LAN, Wireless, NAT, Firewall, VPN, SNMP (selected), Community (sub-selected), Trap, Tools, and Status. The main area has a title bar 'SNMP Community' and a descriptive paragraph about SNMP communities. Below the text is a table with 5 rows for community configuration. The first two rows are pre-filled with 'public' and 'private' community names, both set to 'Read' access and marked as 'Valid'. The remaining three rows are empty for user input. At the bottom right are buttons for HELP, APPLY, and CANCEL.

No.	Community	Access	Valid
1	public	Read	☒
2	private	Write	☒
3		Read	☐
4		Read	☐
5		Read	☐

Community: A community name authorized for management access.

Access: Management access is restricted to Read only or Read/Write.

Valid: Sets administrative status of entry to enabled or disabled.

Note: Up to 5 community names may be entered.

Trap

The screenshot shows the 'Advanced Setup' page for SMC Networks. The left sidebar contains a navigation menu with options: System, WAN, LAN, Wireless, NAT, Firewall, VPN, SNMP, Community, Trap (highlighted), Tools, and Status. The main content area is titled 'SNMP Trap' and includes a descriptive paragraph: 'In the context of SNMP, an unsolicited message can be sent by an agent to management station. The purpose is to notify the management station of some unusual event.' Below this is a table with 5 rows for configuring traps. Each row has columns for 'No.', 'IP Address' (with four input fields for octets), 'Community', and 'Version' (a dropdown menu). All 'Version' dropdowns are currently set to 'Disabled'. At the bottom right of the table are three buttons: 'HELP', 'APPLY', and 'CANCEL'.

No.	IP Address	Community	Version
1	0 . 0 . 0 . 0		Disabled
2	0 . 0 . 0 . 0		Disabled
3	0 . 0 . 0 . 0		Disabled
4	0 . 0 . 0 . 0		Disabled
5	0 . 0 . 0 . 0		Disabled

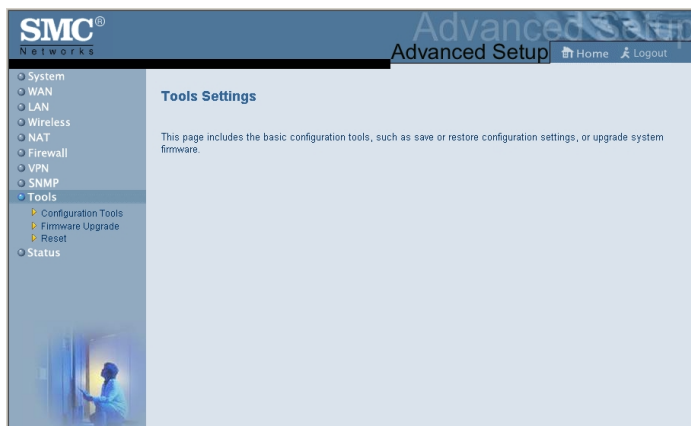
IP Address: IP address of the trap manager.

Community: A community specified for trap management.

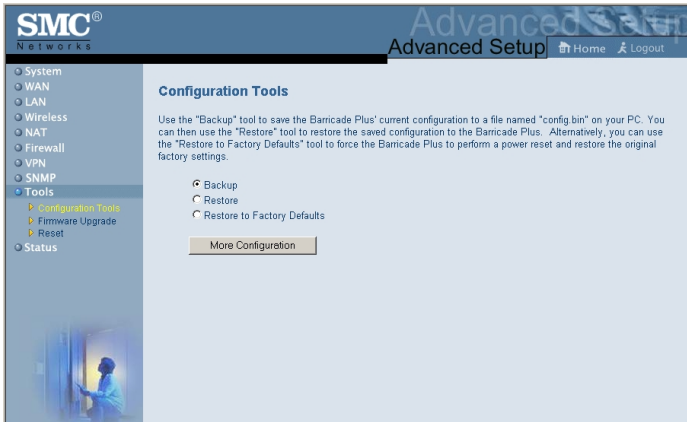
Version: Sets trap status of entry to disabled, or enabled with V1 or V2c.

Tools

You can use the “Tools” menu to restore factory settings, update firmware, or reboot the Wireless Barricade Plus.

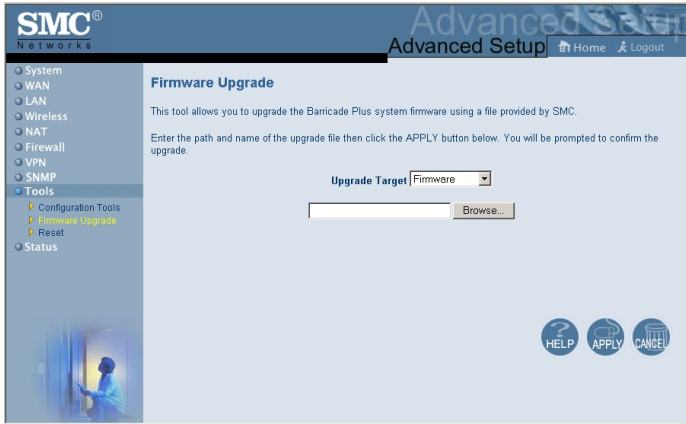


Configuration Tools



The “Backup” option allows you to save your Wireless Barricade Plus’ configuration to a file named `config.bin` on your PC. You can then click on the “Restore” radio button to restore the saved backup configuration file. Selecting the “Restore to Factory Defaults” can restore the factory settings.

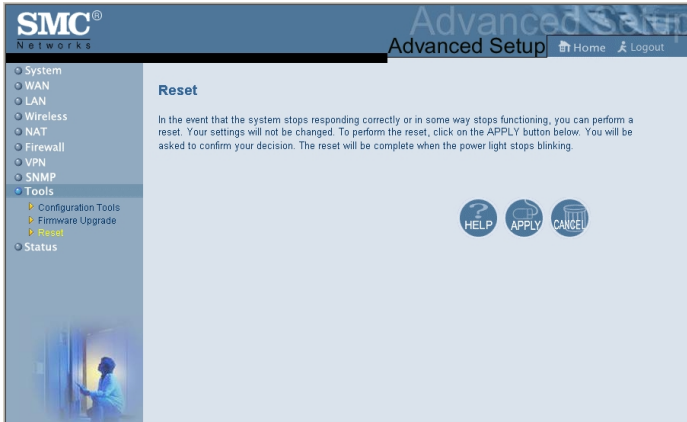
Firmware Upgrade



Use this screen to update the latest firmware using a file provided by SMC.

Note: For latest firmware version information, visit SMC's Web site at <http://www.smc.com>.

Reset

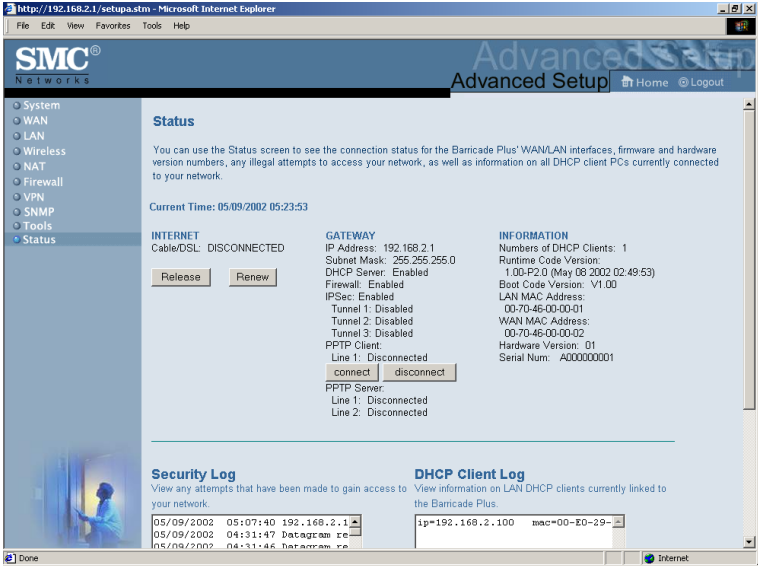


If the Wireless Barricade Plus stops responding, you can click on the “Apply” button to refresh the gateway. The saved configurations of the Wireless Barricade Plus will not be changed back to factory default settings after resetting the gateway.

Note: If you use the reset button on the rear panel, the Wireless Barricade Plus performs a power reset and restores the factory settings.

Status

You can use the following screen to display WAN/LAN connection status, firmware and hardware version numbers, as well as information on all DHCP clients connected to your network.



The following items are included in this screen:

Field	Description
INTERNET	Displays WAN connection type and status.
GATEWAY	Displays system IP settings, as well as DHCP, NAT, PPTP Client and PPTP Server Firewall.
INFORMATION	Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, as well as the hardware version and serial number.
Release	Click on this button to disconnect from the Internet.
Renew	Click on this button to reconnect to the Internet via cable/DSL modem.
Security Log	Displays any illegal attempts to access your network.
DHCP Client Log	Displays information on all DHCP clients on your network.

CHAPTER 5

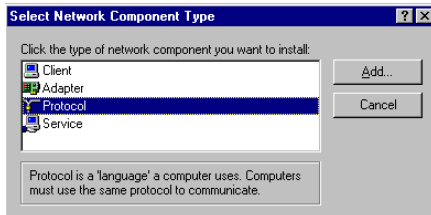
CONFIGURING CLIENT TCP/IP

If you have not previously installed the TCP/IP protocol on your client PCs, refer to the following section. If you need information on how to configure a TCP/IP address on a PC, refer to “Setting TCP/IP to Work with the Wireless Barricade Plus” on page 5-5.

Installing TCP/IP Protocol in Your PC

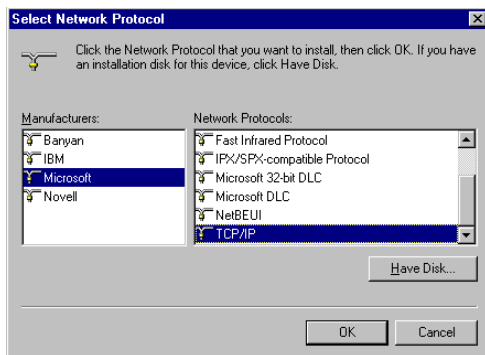
Windows 95/98/ME

1. Click the “Start” button and choose “Settings,” then click “Control Panel.”
2. Double click the “Network” icon and select the “Configuration” tab in the Network window.
3. Click the “Add” button to add the network component to your PC.
4. Double click “Protocol” to add the TCP/IP protocol.



INSTALLING TCP/IP PROTOCOL IN YOUR PC

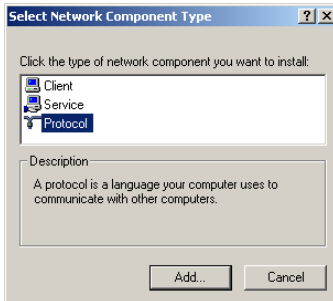
5. Select the “Microsoft” item in the manufacturers list. And choose “TCP/IP” in the Network Protocols. Click the “OK” button to return to the Network window.



6. The TCP/IP protocol will be listed in the Network window. Click “OK” to complete the install procedure and restart your PC to enable the TCP/IP protocol.

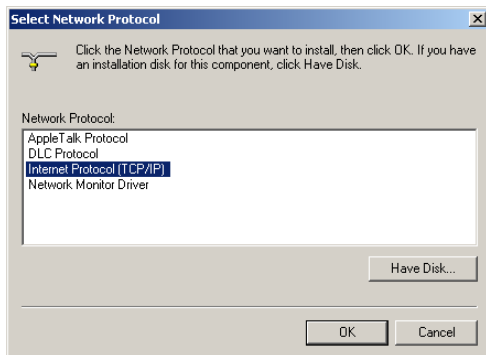
Windows 2000

1. Click the “Start” button and choose “Settings,” then click “Control Panel.”
2. Double click the “Network and Dial-up Connections” icon, then “Local Area Connection” icon, and press the “Properties” button in the “General” tab.
3. Click the “install...” button to add the network component to your PC.
4. Double click on “Protocol” to add the TCP/IP protocol.



INSTALLING TCP/IP PROTOCOL IN YOUR PC

5. Choose “Internet Protocol (TCP/IP)” in the Network Protocols. Click the “OK” button to return to the Network window.

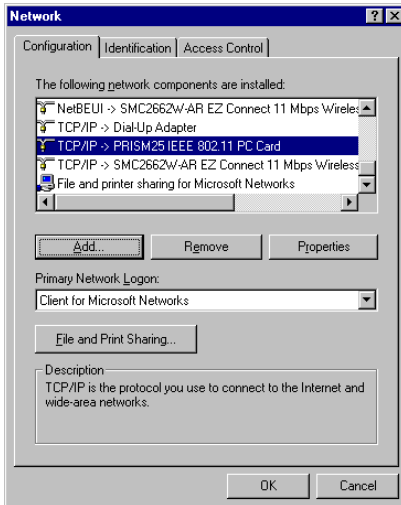


6. The TCP/IP protocol will be listed in the Network window. Click “OK” to complete the install procedure.

Setting TCP/IP to Work with the Wireless Barricade Plus

Windows 95/98/ME

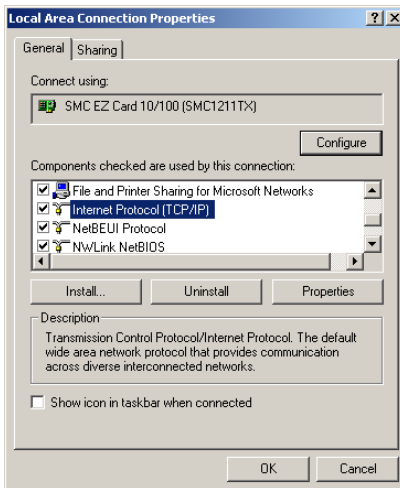
1. Click the “Start” button and choose “Settings,” then click “Control Panel.”
2. Double click the “Network” icon. Select the TCP/IP line that has been assigned to your network card in the “Configuration” tab of the Network window.
3. Click the “Properties” button to set the TCP/IP protocol for the Wireless Barricade Plus.



4. You can dynamically assign TCP/IP address settings to a client, or you can manually configure a client with address settings to meet your specific network requirements. (Note that the default IP address of the Wireless Barricade Plus is 192.168.2.1.)

Windows 2000

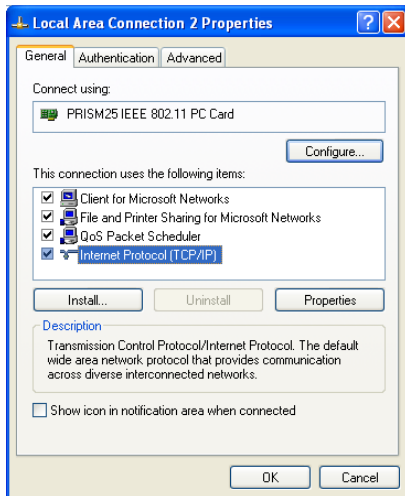
1. Click the “Start” button and choose “Settings,” then click “Control Panel.”
2. Double click the “Network and Dial-up Connections” icon, then “Local Area Connection” icon, and press the “Properties” button in the “General” tab.
3. Select the TCP/IP line that has been assigned to your network card in the “Local Area Connection Properties” window.
4. Click the “Properties” button to set the TCP/IP protocol for the Wireless Barricade Plus.



5. You can dynamically assign TCP/IP address settings to a client, or you can manually configure a client with address settings to meet your specific network requirements. (Note that the default IP address of the Wireless Barricade Plus is 192.168.2.1.)

Windows XP

1. Click the “start” button and choose “Control Panel.”
2. Select the “Network and Internet Connections” icon, then click the “Network Connections” icon, and double click on the “LAN or High-Speed Internet.”
3. Press the “Properties” button in the “General” tab.
4. Select the TCP/IP line that has been assigned to your network card in the “Local Area Connection Properties” window.
5. Click the “Properties” button to set the TCP/IP protocol for the Wireless Barricade Plus.



6. You can dynamically assign TCP/IP address settings to a client, or you can manually configure a client with address settings to meet your specific network requirements. (Note that the default IP address of the Wireless Barricade Plus is 192.168.2.1.)

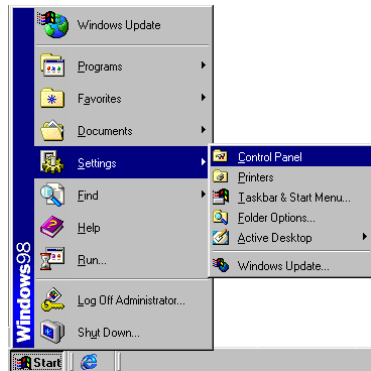
Configuring Your Computer with Windows 95/98/ME

You may find that the instructions here do not exactly match your version of Windows. This is because these steps and screenshots were created from Windows 98. Windows 95 and Windows Millennium Edition are very similar, but not identical, to Windows 98.

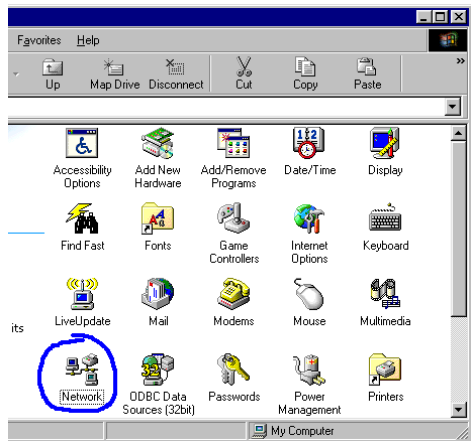
Step 1. Configure TCP/IP Settings

After you have completed the hardware setup by connecting your devices, you need to configure your computer to connect to your Wireless Barricade Plus. You need to determine how your ISP issues your IP address. Many ISPs issue these numbers automatically using a networking technology known as Dynamic Host Configuration Protocol, or DHCP. Other ISPs will specify your IP address and associated numbers, which you must enter manually. This is also known as a static IP address. How your ISP assigns your IP address determines how you will configure your computer.

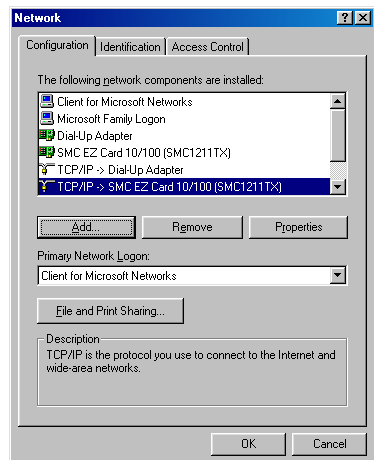
1. From the Windows desktop, click the "Start" button. Choose "Settings," then click "Control Panel."



2. From "Control Panel," double-click the "Network" icon.



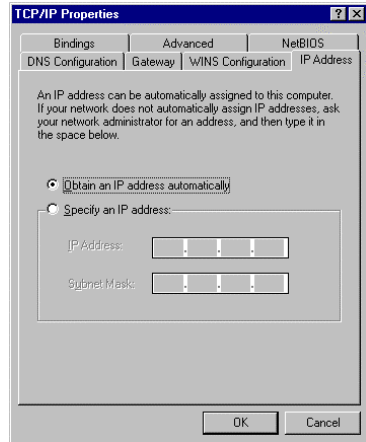
3. In the "Network" window, under the "Configuration" tab, double-click the "TCP/IP" entry that is listed with your network card.



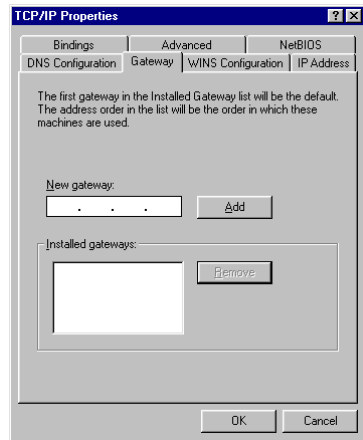
SETTING TCP/IP TO WORK WITH THE WIRELESS BARRICADE PLUS

4. Select the "IP Address" tab.

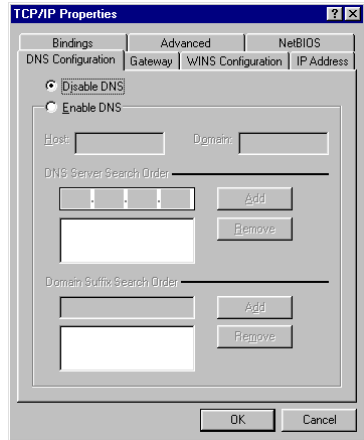
If "Obtain an IP address automatically" is already selected, your computer is already configured for DHCP. Click "Cancel" to close each window, and skip to Step 2 "Disable HTTP Proxy."



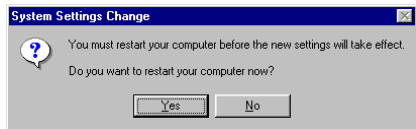
5. Locate your IP address and Subnet Mask. Record them in the spaces provided below.
6. Click the "Gateway" tab and record the numbers listed under "Installed gateways."



7. Click the "DNS Configuration" tab. Locate the DNS servers listed under "DNS Server Search Order." Record the listed addresses.
8. After writing down your settings, check to make sure you have recorded them correctly. Click the "IP Address" tab and then click "Obtain an IP address automatically." Click OK.



9. Windows may need your Windows 95/98/ME CD to copy some files. After it finishes copying, it will then prompt you to restart your system. Click "Yes" and your computer will shut down and restart.



TCP/IP Configuration Setting

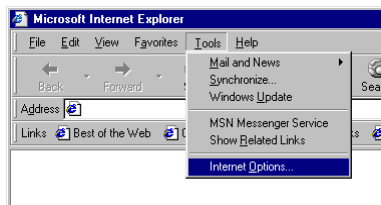
IP Address	_____
Subnet Mask	_____
Primary DNS Server	_____
Secondary DNS Server	_____
Default Gateway	_____

Step 2. Disable HTTP Proxy

You will need to verify that the "HTTP Proxy" feature of your Web browser is disabled. This is so that your Web browser will be able to view the configuration pages inside your Wireless Barricade Plus. The following steps are for Internet Explorer and for Netscape. Determine which browser you use and follow the appropriate steps.

Internet Explorer

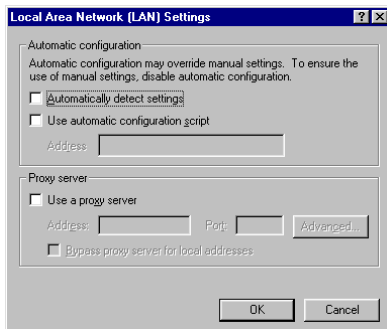
1. Open Internet Explorer and click the stop button. Click "Tools," then "Internet Options."



2. In the "Internet Options" window click the "Connections" tab. Next, click the "LAN Settings..." button.

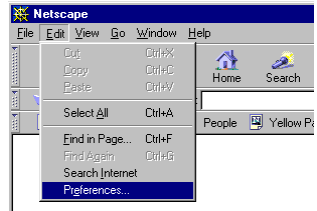


4. Click "OK," and then click "OK" again to close the "Internet Options" window.

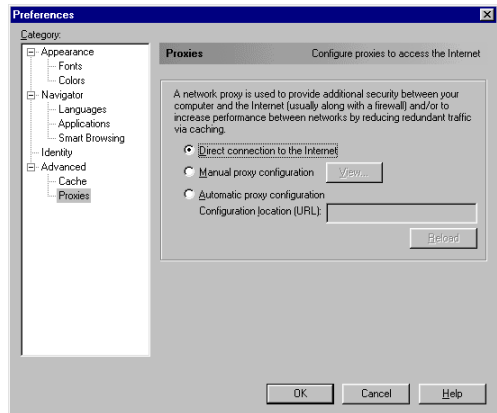


Netscape

1. Open Netscape and click the stop button. Click "Edit," then click "Preferences..."



2. In the "Preferences" window, under "Category" double-click "Advanced," then click "Proxies." Select "Direct connection to the Internet." Click "OK."



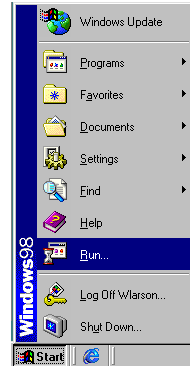
3. Repeat these steps for each Windows 95/98/Me computer connected to your Wireless Barricade Plus.

Step 3. Obtain IP Settings from Your Wireless Barricade Plus

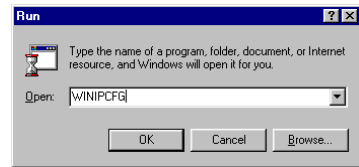
Now that you have configured your computer to connect to your Wireless Barricade Plus, it needs to obtain new network settings. By releasing any old IP settings and renewing them with settings from your Wireless Barricade Plus, you will also verify that you have configured your computer correctly.

SETTING TCP/IP TO WORK WITH THE WIRELESS BARRICADE PLUS

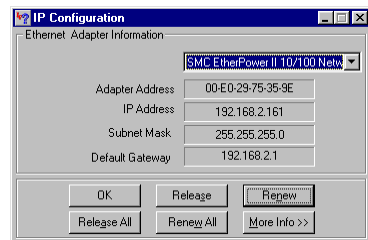
1. Click "Start," then "Run..."



2. Type "WINIPCFG" and click "OK." It may take a minute or two for the "IP Configuration" window to appear.



3. From the drop-down menu, select your network card. Click "Release" and then "Renew." Verify that your IP address is now 192.168.2.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168. 2.1. These values confirm that your Wireless Barricade Plus is functioning. Click "OK" to close the "IP Configuration" window.



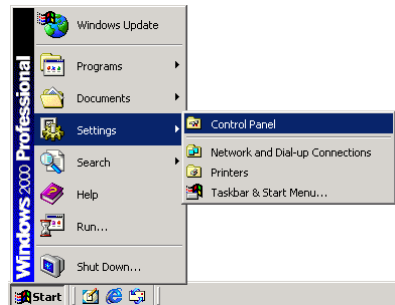
Configuring Your Computer with Windows 2000

Step 1. Configure TCP/IP Settings

After you have completed the hardware setup, you need to configure your computer to connect to your Wireless Barricade Plus. You also need to determine how your ISP issues your IP address. Many ISPs issue these numbers automatically, using a networking technology known as Dynamic Host Configuration Protocol, or DHCP. Other ISPs will specify your IP address and associated numbers, which you must enter manually. This is also known as a static IP address. How your ISP assigns your IP address determines how you will configure your computer.

Here is what to do:

1. From the Windows desktop, click the "Start" button. Choose "Settings," then click "Control Panel."

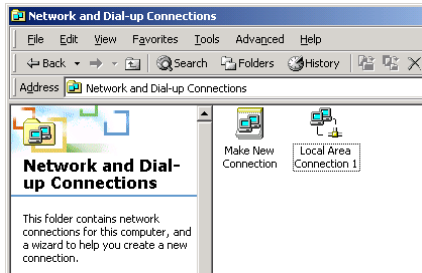


SETTING TCP/IP TO WORK WITH THE WIRELESS BARRICADE PLUS

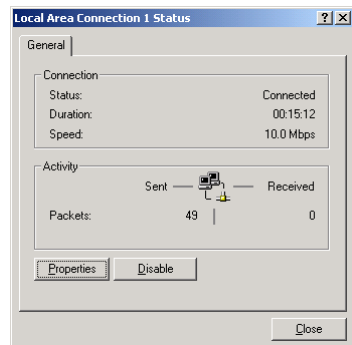
2. Double-click the "Network & Dial-Up Connections" icon.



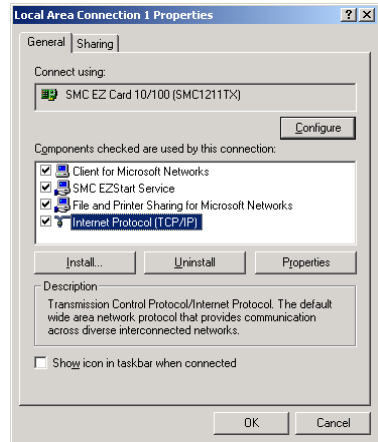
3. Double-click the icon that corresponds to the connection to your Wireless Barricade Plus.



4. Click "Properties."

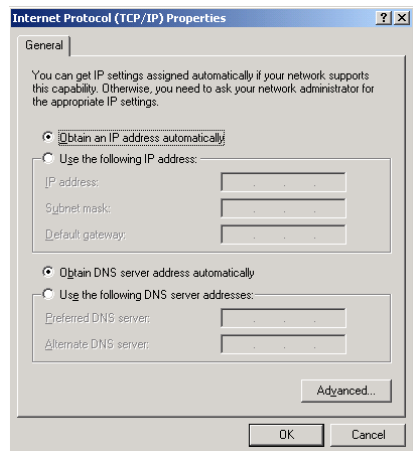


5. Double-click "Internet Protocol (TCP/IP)."



6. All the information that you need to record is on the "Internet Protocol (TCP/IP) Properties" dialog box. Use the spaces below to record the information.

If "Obtain an IP address automatically" and "Obtain DNS server address automatically" are already selected, your computer is already configured for DHCP. Click "Cancel" to close each window, and skip to Step 2 "Disable HTTP Proxy."



SETTING TCP/IP TO WORK WITH THE WIRELESS BARRICADE PLUS

7. Select "Obtain an IP address automatically" and then select "Obtain DNS server address automatically." Then click "OK." Click "OK" or "Close" to close each window.

TCP/IP Configuration Setting

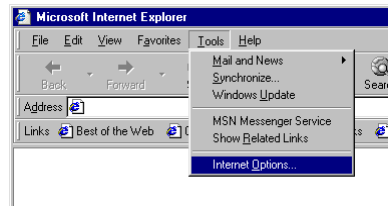
IP Address	_____
Subnet Mask	_____
Primary DNS Server	_____
Secondary DNS Server	_____
Default Gateway	_____

Step 2. Disable HTTP Proxy

You will need to verify that the "HTTP Proxy" feature of your Web browser is disabled. This is so that your Web browser will be able to view the configuration pages inside your Wireless Barricade Plus. The following steps are for Internet Explorer and for Netscape. Determine which browser you use and follow the appropriate steps.

Internet Explorer

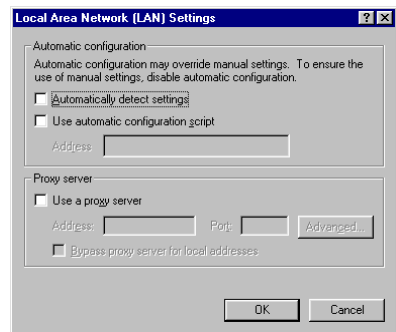
1. Open Internet Explorer and click the stop button. Click "Tools," then "Internet Options."



2. In the "Internet Options" window click the "Connections" tab. Next, click the "LAN Settings..." button.

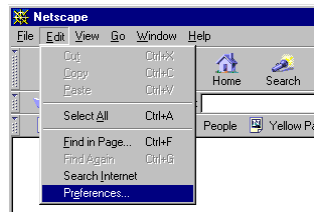


3. Clear all the checkboxes.
4. Click "OK," and then click "OK" again to close the "Internet Options" window.



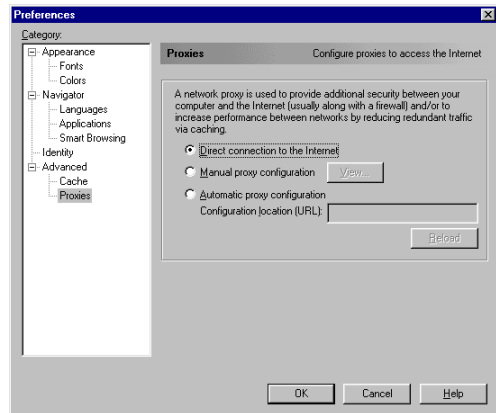
Netscape

1. Open Netscape and click the stop button. Click "Edit," then click "Preferences..."



SETTING TCP/IP TO WORK WITH THE WIRELESS BARRICADE PLUS

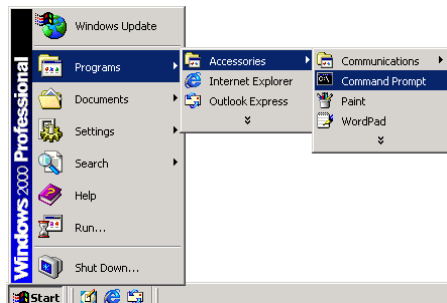
2. In the "Preferences" window, under "Category" double-click "Advanced," then click "Proxies." Select "Direct connection to the Internet." Click "OK."



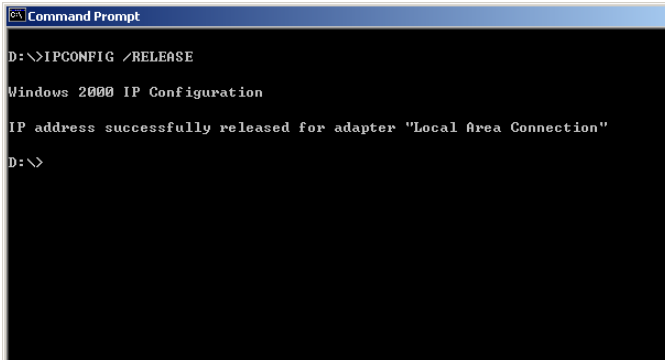
Step 3. Obtain IP Settings From Your Wireless Barricade Plus

Now that you have configured your computer to connect to your Wireless Barricade Plus, it needs to obtain new network settings. By releasing any old IP settings and renewing them with settings from your Wireless Barricade Plus, you will also verify that you have configured your computer correctly.

1. From the Windows desktop, click the "Start" button, then "Programs," then "Accessories," and then click "Command Prompt."



2. In the "Command Prompt" window, type "IPCONFIG /RELEASE" and press the <ENTER> key.



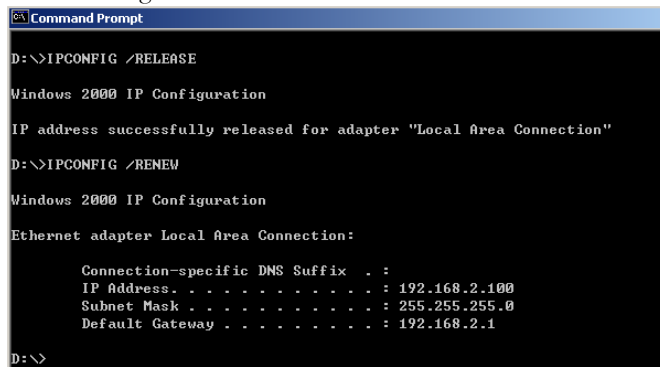
```
Command Prompt
D:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection"

D:\>
```

3. Type "IPCONFIG /RENEW" and press the <ENTER> key. Verify that your IP address is now 192.168.2.xxx (2-255), your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.2.1. These values confirm that your Wireless Barricade Plus is functioning.



```
Command Prompt
D:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection"

D:\>IPCONFIG /RENEW

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

D:\>
```

Type "EXIT" and press <ENTER> to close the "Command Prompt" window.

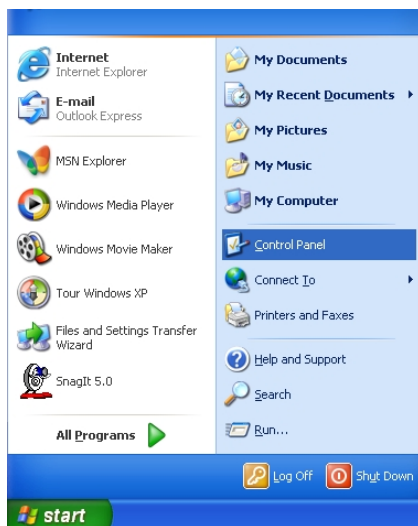
Configuring Your Computer with Windows XP

Step 1. Configure TCP/IP Settings

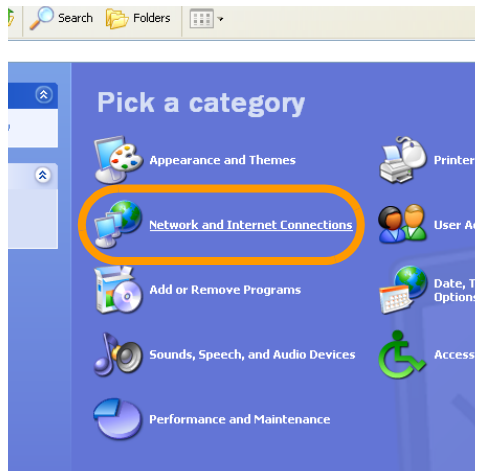
After you have completed the hardware setup, you need to configure your computer to connect to your Wireless Barricade Plus. You also need to determine how your ISP issues your IP address. Many ISPs issue these numbers automatically, using a networking technology known as Dynamic Host Configuration Protocol, or DHCP. Other ISPs will specify your IP address and associated numbers, which you must enter manually. This is also known as a static IP address. How your ISP assigns your IP address determines how you will configure your computer.

Here is what to do:

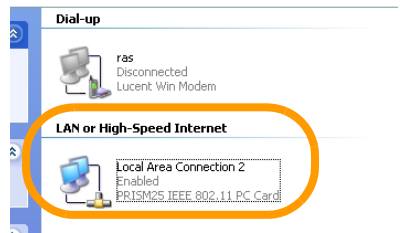
1. From the Windows desktop, click the "start" button. Choose "Control Panel."



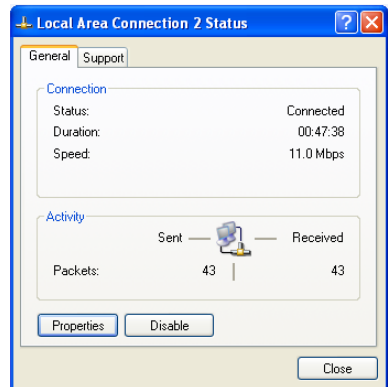
2. Select the “Network and Internet Connections” icon, then click the “Network Connections” icon.



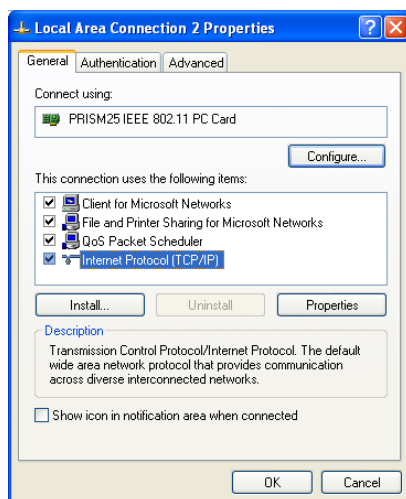
3. Double click on the “LAN or High-Speed Internet.”



4. Click "Properties."

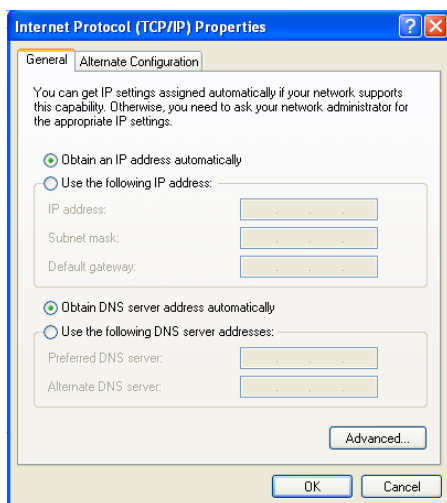


5. Double-click "Internet Protocol (TCP/IP)."



6. All the information that you need to record is on the "Internet Protocol (TCP/IP) Properties" dialog box. Use the spaces below to record the information.

If "Obtain an IP address automatically" and "Obtain DNS server address automatically" are already selected, your computer is already configured for DHCP. Click "Cancel" to close each window, and skip to Step 2 "Disable HTTP Proxy."



7. Select "Obtain an IP address automatically" and then select "Obtain DNS server address automatically." Then click "OK." Click "OK" or "Close" to close each window.

TCP/IP Configuration Setting

IP Address	____.____.____.____
Subnet Mask	____.____.____.____
Primary DNS Server	____.____.____.____
Secondary DNS Server	____.____.____.____
Default Gateway	____.____.____.____

Step 2. Disable HTTP Proxy

You will need to verify that the "HTTP Proxy" feature of your Web browser is disabled. This is so that your Web browser will be able to view the configuration pages inside your Wireless Barricade Plus. The following steps are for Internet Explorer and for Netscape. Determine which browser you use and follow the appropriate steps.

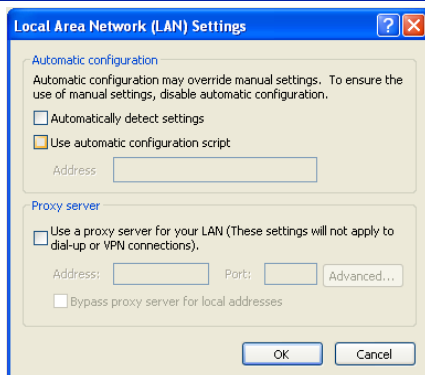
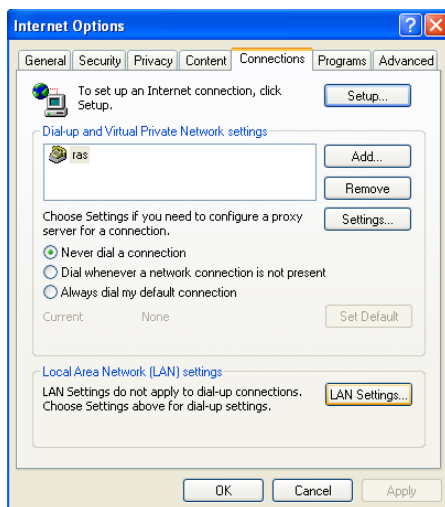
Internet Explorer

1. Open Internet Explorer and click the stop button. Click "Tools," then "Internet Options."



SETTING TCP/IP TO WORK WITH THE WIRELESS BARRICADE PLUS

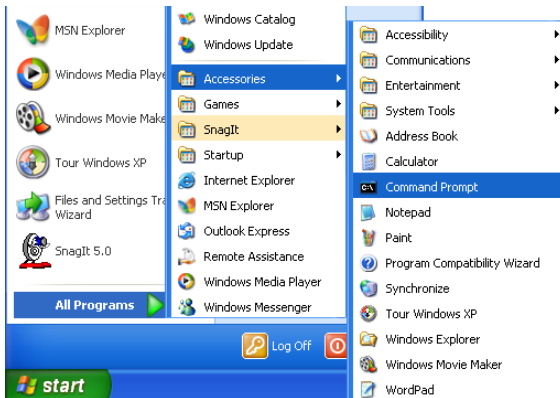
2. In the "Internet Options" window click the "Connections" tab. Next, click the "LAN Settings..." button.
3. Clear all the checkboxes.
4. Click "OK," and then click "OK" again to close the "Internet Options" window.



Step 3. Obtain IP Settings From Your Wireless Barricade Plus

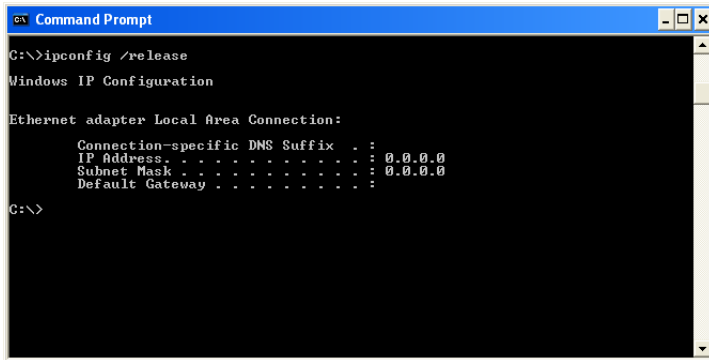
Now that you have configured your computer to connect to your Wireless Barricade Plus, it needs to obtain new network settings. By releasing any old IP settings and renewing them with settings from your Wireless Barricade Plus, you will also verify that you have configured your computer correctly.

1. From the Windows desktop, click the "Start" button, then "Programs," then "Accessories," and then click "Command Prompt."



SETTING TCP/IP TO WORK WITH THE WIRELESS BARRICADE PLUS

2. In the "Command Prompt" window, type "IPCONFIG /RELEASE" and press the <ENTER> key.



```
Command Prompt
C:\>ipconfig /release

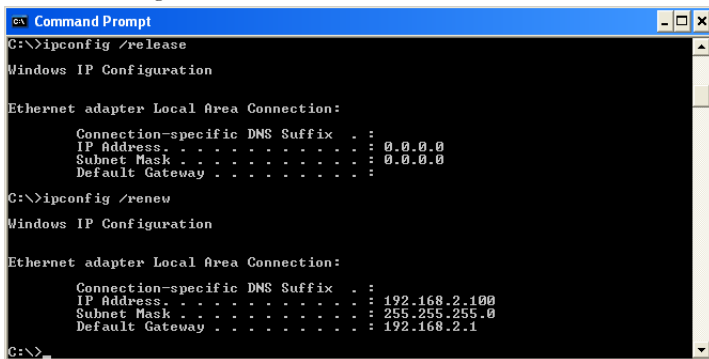
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

C:\>
```

3. Type "IPCONFIG /RENEW" and press the <ENTER> key. Verify that your IP address is now 192.168.2.xxx (2-255), your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.2.1. These values confirm that your Wireless Barricade Plus is functioning.



```
Command Prompt
C:\>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

C:\>ipconfig /renew

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

C:\>
```

Type "EXIT" and press <ENTER> to close the "Command Prompt" window.

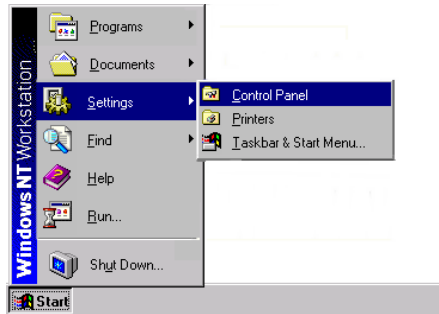
Configuring Your Computer with Windows NT 4.0

Step 1. Configure TCP/IP Settings

After you have completed the hardware setup, you need to configure your computer to connect to your Wireless Barricade Plus. You need to determine how your ISP issues your IP address. Many ISPs issue these numbers automatically using a networking technology known as Dynamic Host Configuration Protocol, or DHCP. Other ISPs will specify your IP address and associated numbers, which you must enter manually. This is also known as a static IP address. How your ISP assigns your IP address determines how you will configure your computer.

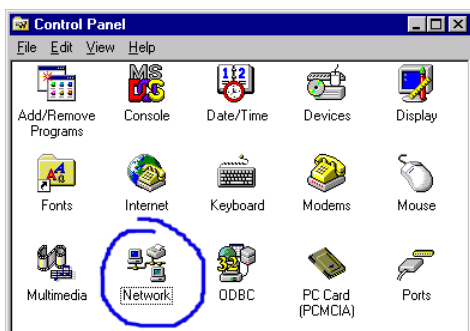
Here is what to do:

1. From the Windows desktop click "Start," then "Settings," and click "Control Panel."

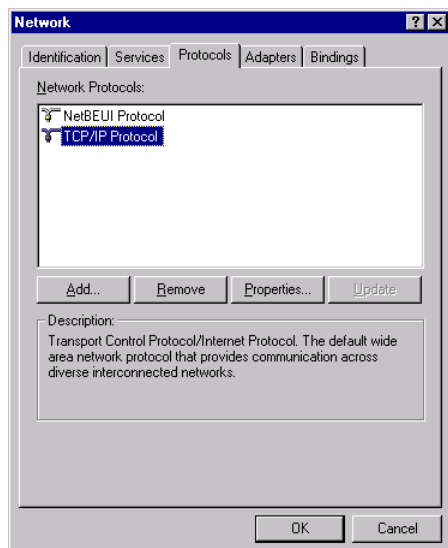


SETTING TCP/IP TO WORK WITH THE WIRELESS BARRICADE PLUS

2. Double-click the "Network" icon.

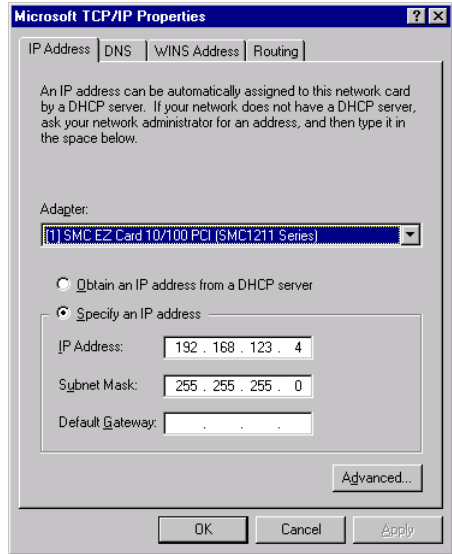


3. Select the "Protocols" tab.
4. Double-click "TCP/IP Protocol."

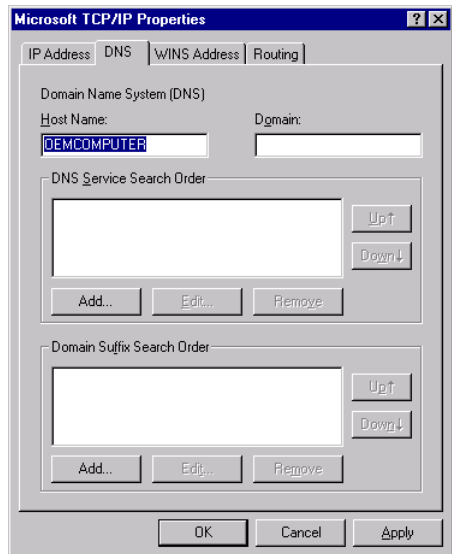


5. Select the "IP Address" tab.
6. In the "Adapter" drop-down list, be sure your Ethernet adapter is selected.

If "Obtain an IP address automatically" is already selected, your computer is already configured for DHCP. Click "Cancel" to close each window, and skip to Step 2 "Disable HTTP Proxy."



7. In the "TCP/IP Properties" dialog box, click the IP address tab to locate your IP address, Subnet Mask, and Default Gateway. Record these values in the space provided below.
8. Click the "DNS" tab to see the primary and secondary DNS servers. Record these values in the appropriate spaces below.



SETTING TCP/IP TO WORK WITH THE WIRELESS BARRICADE PLUS

9. After writing down your IP settings, click the IP address tab. Select "Obtain IP address automatically" and click OK. Click OK again to close the "Network" window.
10. Windows may copy some files, and will then prompt you to restart your system. Click "Yes" and your computer will shut down and restart.

TCP/IP Configuration Setting

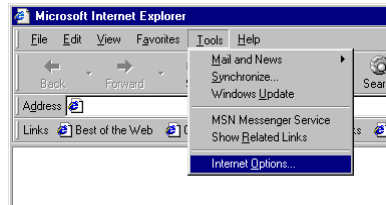
IP Address	_____
Subnet Mask	_____
Primary DNS Server	_____
Secondary DNS Server	_____
Default Gateway	_____

Step 2. Disable HTTP Proxy

You will need to verify that the "HTTP Proxy" feature of your Web browser is disabled. This is so that your Web browser will be able to view the configuration pages inside your Wireless Barricade Plus. The following steps are for Internet Explorer and for Netscape. Determine which browser you use and follow the appropriate steps.

Internet Explorer

1. Open Internet Explorer and click the stop button. Click "Tools," then "Internet Options."

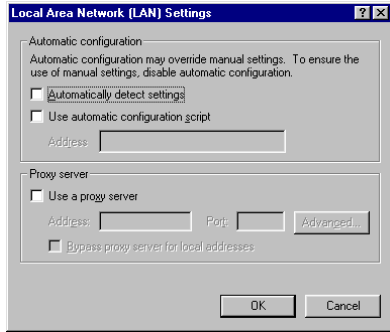


2. In the "Internet Options" window click the "Connections" tab. Next, click the "LAN Settings..." button.



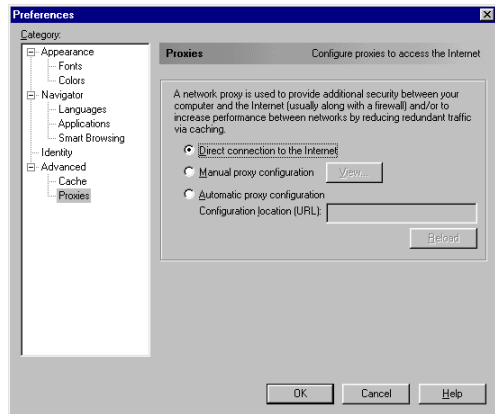
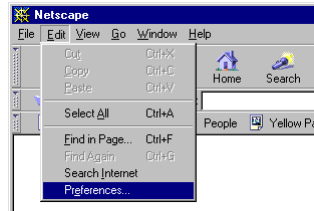
SETTING TCP/IP TO WORK WITH THE WIRELESS BARRICADE PLUS

3. Clear all the checkboxes.
4. Click "OK," and then click "OK" again to close the "Internet Options" window.



Netscape

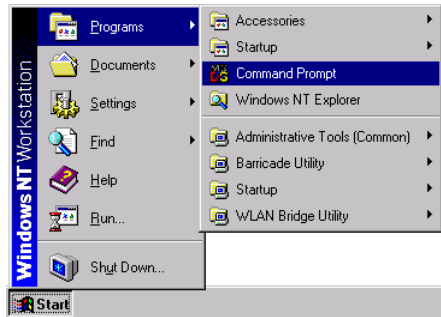
1. Open Netscape and click the stop button. Click "Edit," then click "Preferences..."
2. In the "Preferences" window, under "Category," double-click "Advanced," then click "Proxies." Select "Direct connection to the Internet." Click "OK."



Step 3. Obtain IP Settings From Your Wireless Barricade Plus

Now that you have configured your computer to connect to your Wireless Barricade Plus, it needs to obtain new network settings. By releasing any old IP settings and renewing them with settings from your Wireless Barricade Plus, you will also verify that you have configured your computer correctly.

1. From the Windows desktop, click the "Start" button, then "Programs," and then select "Command Prompt."
2. In the "Command Prompt" window, type "IPCONFIG /RELEASE" and press the <ENTER> key.



```

C:\> Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

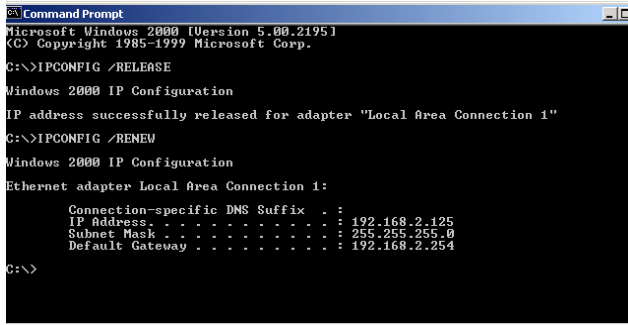
C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection 1"

C:\>_
```

3. Type "IPCONFIG /RENEW" and press the <ENTER> key. Verify that your IP address is now 192.168.2.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.2.1. These values confirm that your Wireless Barricade Plus is functioning.



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection 1"

C:\>IPCONFIG /RENEW

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 1:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.2.125
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.254

C:\>
```

4. Type "EXIT" and press <ENTER> to close the "Command Prompt" window.

Configuring Your Macintosh Computer

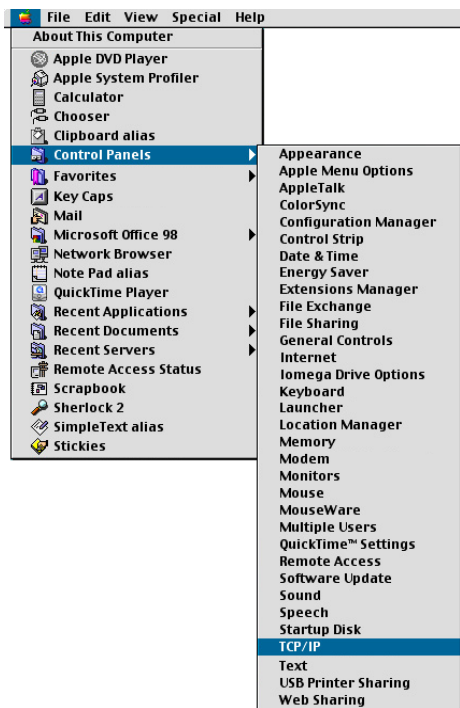
You may find that the instructions here do not exactly match your screen. This is because these steps and screenshots were created using Mac OS 8.5. Mac OS 7.x and above are all very similar, but may not be identical to Mac OS 8.5.

Step 1. Configure TCP/IP Settings

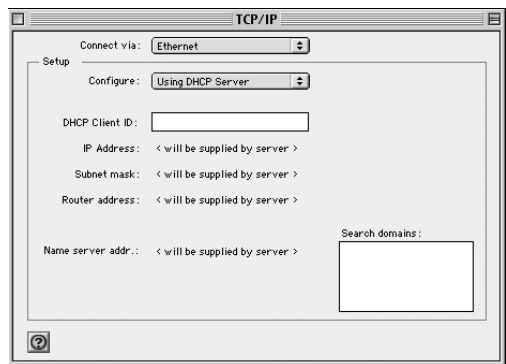
After you have completed the hardware setup, you need to configure your computer to connect to your Wireless Barricade Plus. You need to determine how your ISP issues your IP address. Many ISPs issue these numbers automatically using a networking technology known as Dynamic Host Configuration Protocol, or DHCP. Other ISPs will specify your IP address and associated numbers, which you must enter manually. This is also known as a static IP address. How your ISP assigns your IP address determines how you will configure your computer.

Here is what to do:

1. Pull down the Apple Menu. Click "Control Panels" and select TCP/IP.

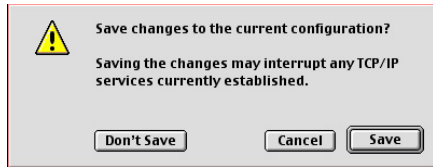


2. In the TCP/IP dialog box, make sure that "Ethernet" is selected in the "Connect Via:" field.



If "Using DHCP Server" is already selected in the "Configure" field, your computer is already configured for DHCP. Close the TCP/IP dialog box, and skip to Step 2 "Disable HTTP Proxy."

3. All the information that you need to record is on the "TCP/IP" dialog box. Use the space below to record the information.
4. After writing down your IP settings, select "Using DHCP Server" in the "Configure" field and close the window.
5. Another box will appear asking whether you want to save your TCP/IP settings. Click Save.



TCP/IP Configuration Setting

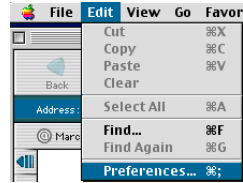
IP Address	_____
Subnet Mask	_____
Router	_____
Name Server	_____

Step 2. Disable HTTP Proxy

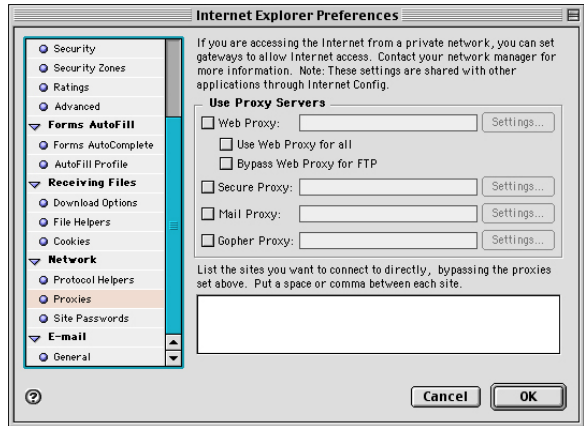
You will need to verify that the "HTTP Proxy" feature of your Web browser is disabled. This is so that your Web browser will be able to view the configuration pages inside your Wireless Barricade Plus. The following steps are for Internet Explorer and for Netscape. Determine which browser you use and follow the appropriate steps.

Internet Explorer

1. Open Internet Explorer and click the stop button. Click "Edit" and select "Preferences."



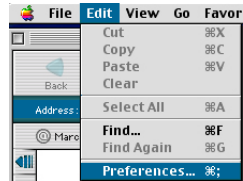
2. In the Internet Explorer Preferences window, under Network, select Proxies.



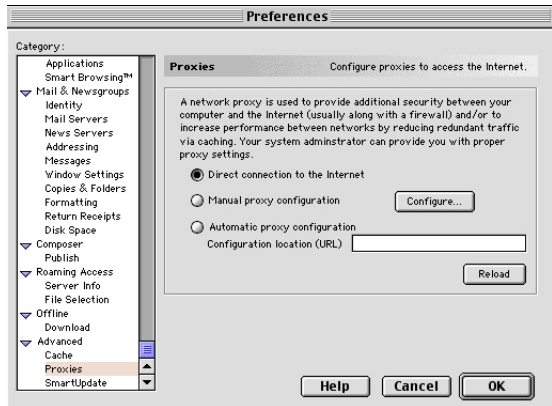
3. Uncheck all checkboxes and click OK.

Netscape

1. Open Netscape and click the stop button. Click "Edit" and select "Preferences."



2. In the "Preferences" dialog box, in the left-hand column labeled "Category," select "Advanced." Under the "Advanced" category, select "Proxies."

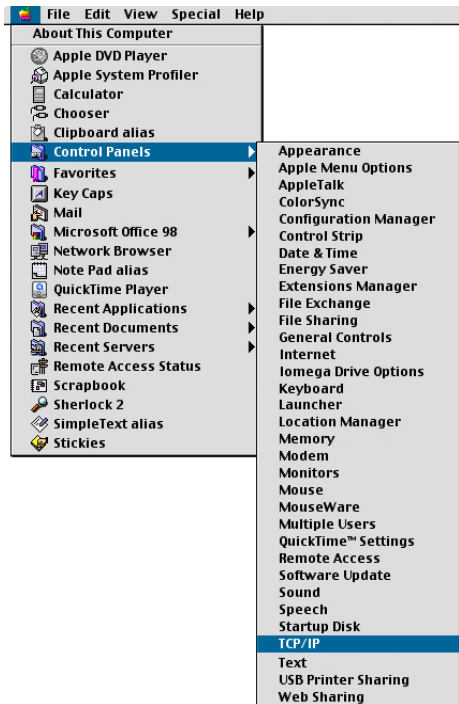


3. Select "Direct Connection to the Internet" and click OK.

Step 3. Obtain IP Settings From Your Wireless Barricade Plus

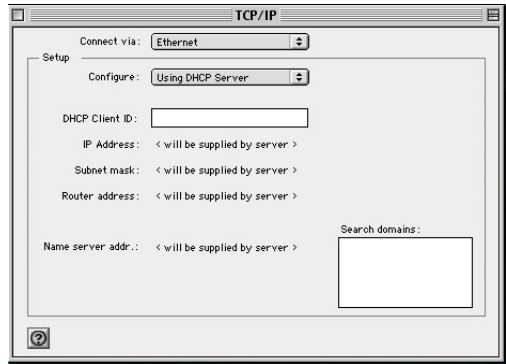
Now that you have configured your computer to connect to your Wireless Barricade Plus, it needs to obtain new network settings. By releasing any old IP settings and renewing them with settings from your Wireless Barricade Plus, you will also verify that you have configured your computer correctly.

1. Pull down the Apple Menu. Click "Control Panels" and select TCP/IP.



SETTING TCP/IP TO WORK WITH THE WIRELESS BARRICADE PLUS

2. In the TCP/IP window, your new settings will be shown. Verify that your IP address is now 192.168.2.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.2.1. These

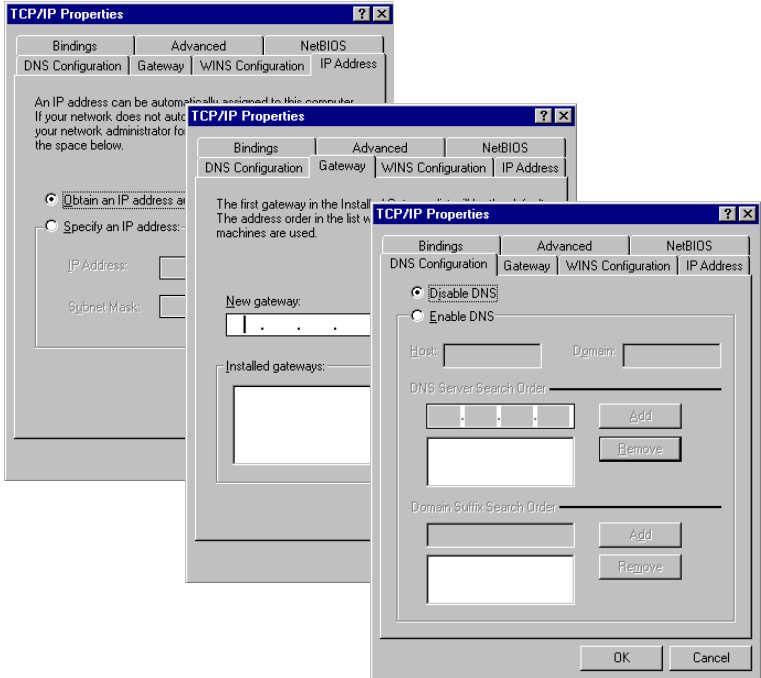


values confirm that your Wireless Barricade Plus is functioning.

3. Close the TCP/IP window.

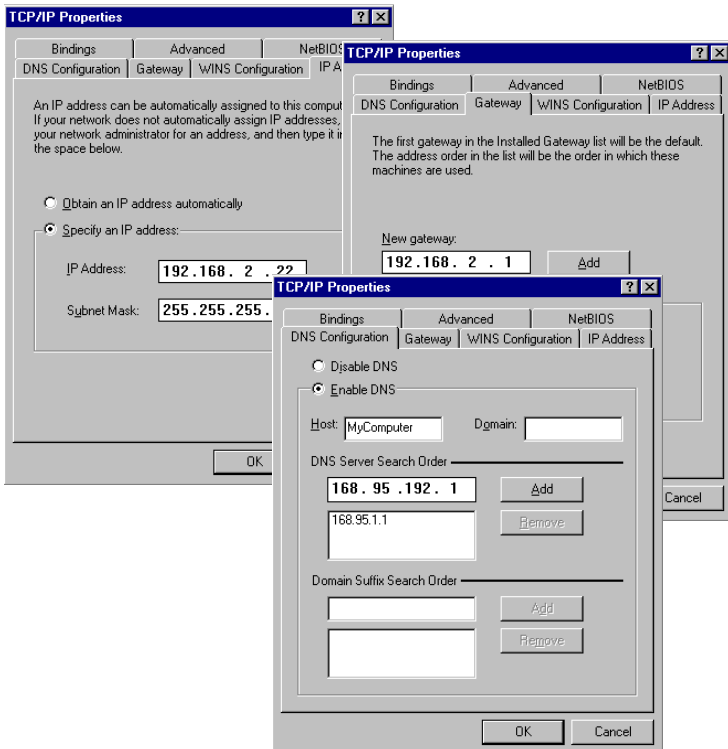
Dynamic IP Allocation via a DHCP Server

Select “Obtain an IP address automatically” in the IP Address tab. Do not input any values under the “Gateway” tab, and choose “Disable DNS” in the “DNS Configuration” tab. These settings will be automatically configured by the DHCP server. Click “OK” and reboot your system to implement the changes.



Manual IP Configuration

1. Select “Specify an IP address” in the “IP Address” tab. Select an IP address based on the default network 192.168.2.X (where X is between 1 and 254), and use 255.255.255.0 for the Subnet Mask.
2. In the “Gateway” tab, add the IP address of the Wireless Barricade Plus (default: 192.168.2.1) in the “New gateway” field and click “Add.”
3. In the “DNS Configuration” tab, add the IP address for the Wireless Barricade Plus and click “Add.” This automatically relays DNS requests to the DNS server(s) provided by your ISP. Otherwise, add specific DNS servers into the “DNS Server Search Order” field and click “Add.”



4. After finishing TCP/IP setup, click “OK,” and then reboot the computer. After that, set up other PCs on the LAN according to the procedures described above.

Verifying Your TCP/IP Connection

After installing the TCP/IP communication protocol and configuring an IP address in the same network with the Wireless Barricade Plus, you can use the “Ping” command to check if your computer is successfully connected to the Wireless Barricade Plus. The following example shows how the Ping procedure can be executed in an MS-DOS window. First, execute the “Ping” command:

```
ping 192.168.2.1
```

If the following messages appear:

```
Pinging 192.168.2.1 with 32 bytes of data:  
Reply from 192.168.2.1: bytes=32 time=2ms TTL=64
```

a communication link between your computer and the Wireless Barricade Plus has been successfully established.

Otherwise, if you get the following messages:

```
Pinging 192.168.2.1 with 32 bytes of data:  
Request timed out.
```

there may be something wrong in your installation procedure. Check the following items in sequence:

1. Is the Ethernet cable correctly connected between the Wireless Barricade Plus and your computer?

The LAN LED on the Wireless Barricade Plus and the Link LED of the network card on your computer must be on.

SETTING TCP/IP TO WORK WITH THE WIRELESS BARRICADE PLUS

2. Is TCP/IP properly configured on your computer?

If the IP address of the Wireless Barricade Plus is 192.168.2.1, the IP address of your PC must be from 192.168.2.2 - 192.168.2.254 and the Default Gateway must be 192.168.2.1.

If you can successfully Ping the Wireless Barricade Plus, then you are now ready to connect to the Internet!

APPENDIX A

TROUBLESHOOTING

This appendix describes common problems you may encounter and possible solutions to them. The Wireless Barricade Plus can be easily monitored through panel indicators to identify problems. If you cannot resolve any connection problems after checking the indicators, then refer to the other sections in the following table.

Troubleshooting Chart	
Symptom	Action
<i>LED Indicators</i>	
Power LED is Off	• External power supply has failed or is disconnected. • Check connections between the Wireless Barricade Plus, the external power supply, and the wall outlet. • If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or external power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses or surges at the power outlet. If you still cannot isolate the problem, then the external power supply may be defective. In this case, contact SMC Technical Support for assistance.

Troubleshooting Chart	
Symptom	Action
<i>LED Indicators</i>	
Link LED is Off	• Verify that the Wireless Barricade Plus and attached device are powered on. • Be sure the cable is plugged into both the Wireless Barricade Plus and the corresponding device. • Verify that the proper cable type is used and that its length does not exceed the specified limits. • Be sure that the network interface on the attached device is configured for the proper communication speed and duplex mode. • Check the adapter on the attached device and cable connections for possible defects. Replace any defective adapter or cable if necessary.
<i>Network Connection Problems</i>	
Cannot Ping the Wireless Barricade Plus from the attached LAN, or the Wireless Barricade Plus cannot Ping any device on the attached LAN	• Verify that the IP addresses are properly configured. For most applications, you should use the Wireless Barricade Plus' DHCP function to dynamically assign IP addresses to any host on the attached LAN. However, if you manually configure any IP addresses on the LAN, verify that the same network address (network component of the IP address) and subnet mask are used for both the Wireless Barricade Plus and any attached LAN devices. • Be sure the device you want to Ping (or from which you are Pinging) has been configured for TCP/IP.
Mobile users cannot access the Wireless Barricade Plus	• Make sure that the Wireless Barricade Plus and all mobile users are configured to use the same radio channel, Service Set Identifier (SSID), and encryption keys. • Ensure that all mobile users are within range of the Wireless Barricade Plus as specified in Appendix C.

Troubleshooting Chart	
Symptom	Action
<i>Management Problems</i>	
Cannot connect using the Web browser	• Be sure to have configured the Wireless Barricade Plus with a valid IP address, subnet mask and default gateway. • Check that you have a valid network connection to the Wireless Barricade Plus and that the port you are using has not been disabled. • Check the network cabling between the management station and the Wireless Barricade Plus.
Forgot or lost the password	• Press the Reset button on the front panel (holding it down for at least five seconds) to restore the factory defaults.

APPENDIX B

CABLES

Ethernet Cable

Specifications

Cable Types and Specifications			
Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm UTP	100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	100 m (328 ft)	RJ-45

Twisted-pair Cable

Caution: DO-NOT plug a phone jack connector into any RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

For 10BASE-T/100BASE-TX connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be red and the other, red with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable. All RJ-45 ports on the SMC7004FW, except for the WAN port, support automatic MDI/MDI-X configuration. This means that you can use straight-through cable to attach the LAN ports to any network device. However, when connecting the WAN port to a broadband modem, you will need to use either straight-through or crossover cable, depending on the port type used on the modem.

Figure B-1 illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

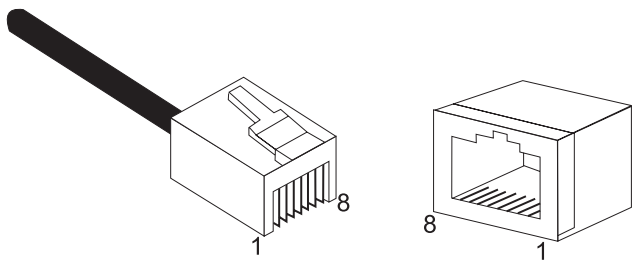


Figure B-1. RJ-45 Connector Pin Numbers

Straight-through Cable

Straight-Through RJ-45 Pin Assignments	
End 1	End 2
1 (TD+)	1 (TD+)
2 (TD-)	2 (TD-)
3 (RD+)	3 (RD+)
6 (RD-)	6 (RD-)

Pins 4, 5, 7 and 8 are not connected.

Crossover Cable

Crossover RJ-45 Pin Assignments	
End 1	End 2
1 (TD+)	3 (RD+)
2 (TD-)	6 (RD-)
3 (RD+)	1 (TD+)
6 (RD-)	2 (TD-)

Pins 4, 5, 7 and 8 are not connected.

RJ-45 Port Pin Assignments

All LAN ports on the Wireless Barricade Plus support automatic MDI/MDI-X configuration. This means that the pin signals in use will depend on whether the LAN port is operating in MDI or MDI-X mode. However, the WAN port is configured only for MDI-X mode.

Pin	MDI Signal Name*	MDI-X Signal Name*
1	Transmit Data (TD+)	Receive Data (RD+)
2	Transmit Data (TD-)	Receive Data (RD-)
3	Receive Data (RD+)	Transmit Data (TD+)
6	Receive Data (RD-)	Transmit Data (RD-)

Pins 4, 5, 7 and 8 are not connected.

* The “+” and “-” signs represent the polarity of the wires that make up each wire pair.

CABLES

APPENDIX C

SPECIFICATIONS

LAN Interface

10BASE-T/100BASE-TX
3 RJ-45 ports

WAN Interface

10BASE-T/100BASE-TX, 1 RJ-45 port

WLAN Interface

Standard: IEEE 802.11b, Direct Sequence Spread Spectrum (DSSS)
Transmission Rate: 11 Mbps, automatic fallback to 5.5, 2 or 1 Mbps
Maximum Channels: US/Canada: 11, Europe (ETSI): 13
Range: Up to 304.8m (1000 ft)
Frequency: (US/Canada/Europe) 2.400-2.4835 GHz, Japan: 2.471-2.497 GHz
Sensitivity: 1, 2, 5.5 Mbps: -80 dBm; 11 Mbps: -76 dBm typical
Modulation: CCK, BPSK, QPSK
Encryption: 64-bit/128-bit WEP
Maximum Clients: 128

Indicator Panel

WAN, WLAN, LAN (Link, Activity), Power

Dimensions

19.5 x 11.25 x 2.55 cm (7.68 x 4.43 x 1.00 in)

Weight

1.34 lbs (0.61 kg)

Input Power

9 V (1 A)

SPECIFICATIONS

Maximum Current

0.04A RMS max. @ 110V/240V

Power Consumption

5 Watts max. @ 100-240 VAC

Management

Web management

Advanced Features

Dynamic IP Address Configuration – DHCP, DNS

Firewall – Client privileges, hacker prevention and logging

Virtual Private Network – PPTP, IPSec, VPN tunneling

Stateful Packet Inspection

Internet Standards

ARP (RFC 826), IP (RFC 791), ICMP (RFC 792), UDP (RFC 768),
TCP (RFC 793), Telnet (RFC 854-859), MD5 (RFC 1321), BOOTP
Extension (RFC 1497), PPP LCP Extension (RFC 1570), PPPoE
(RFC 2516), NAT (RFC 1631), HTML (RFC 1866), HTTP (RFC
1945), DHCP (RFC 2131), PPTP (RFC 2637)

Temperature

Operating 32 to 104°F (0 to 40°C)

Storage -40 to 158°F (-40 to 70°C)

Humidity

5% to 95% (noncondensing)

Compliances

CE Mark

Emissions

FCC Class B

VCCI Class B

Industry Canada Class B

EN55022 (CISPR 22) Class B

C-Tick - AS/NZS 3548 (1995) Class B

Immunity

EN 61000-3-2/3

EN 61000-4-2/3/4/5/6/8/11

Safety

UL 1950

EN60950 (TÜV)

CSA 22.2 No. 950

Warranty

Limited Lifetime

SPECIFICATIONS

APPENDIX D

ORDERING INFORMATION

Barricade Plus Broadband Firewall Router Products	
SMC7004FW	4-port Cable/DSL Broadband Router - WAN/LAN
SMC7004WFW	4-port Wireless Cable/DSL Broadband Router - WAN/LAN/WLAN

ORDERING INFORMATION

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)
(800) SMC-4-YOU; (949) 679-8000; Fax: (949) 679-1481
From Europe (8:00 AM - 5:30 PM UK Time)
44 (0) 118 974 8700; Fax: 44 (0) 118 974 8701

INTERNET

E-mail addresses:

techsupport@smc.com
european.techsupport@smc-europe.com

Driver updates:

[http://www.smc.com/index.cfm?action=tech support drivers downloads](http://www.smc.com/index.cfm?action=tech%20support%20drivers%20downloads)

World Wide Web:

<http://www.smc.com/>
<http://www.smc-europe.com/>

FOR LITERATURE OR ADVERTISING RESPONSE, CALL:

U.S.A. and Canada:	(800) SMC-4-YOU;	Fax (949) 679-1481
Spain:	34-93-477-4935;	Fax 34-93-477-3774
UK:	44 (0) 118 974 8700;	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32;	Fax 33 (0) 41 38 01 58
Italy:	39 02 739 12 33;	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88;	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0;	Fax 49 (0) 89 92861-230
Switzerland:	41 (0) 1 9409971;	Fax 41 (0) 1 9409972
Nordic:	46 (0) 868 70700;	Fax 46 (0) 887 62 62
Northern Europe:	44 (0) 118 974 8700;	Fax 44 (0) 118 974 8701
Eastern Europe:	34 -93-477-4920;	Fax 34 93 477 3774
Sub Saharian Africa:	27-11 314 1133;	Fax 27-11 314 9133
North Africa:	34 93 477 4920;	Fax 34 93 477 3774
Russia:	7 (095) 290 29 96;	Fax 7 (095) 290 29 96
PRC:	86-10-6235-4958;	Fax 86-10-6235-4962
Taiwan:	886-2-2659-9669;	Fax 886-2-2659-9666
Asia Pacific:	(65) 238 6556;	Fax (65) 238 6466
Korea:	82-2-553-0860;	Fax 82-2-553-7202
Japan:	81-45-224-2332;	Fax 81-45-224-2331
Australia:	61-2-9416-0437;	Fax 61-2-9416-0474
India:	91-22-8204437;	Fax 91-22-8204443

If you are looking for further contact information, please visit www.smc.com or www.smc-europe.com.

SMC[®]
N e t w o r k s

38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

Model Number: SMC7004WFW
Revision Number: F1.0 E052002-R01
Part Number: 01-111339-006